MAANPUOLUSTUSKORKEAKOULU

LANGATTOMIEN LÄHIVERKKOJEN SUOJAUS MAANTIETUKIKOHTAYMPÄRISTÖSSÄ

Pro Gradu -tutkielma
Yliluutnantti
Ville Paukku
SMOHJ11
Ilmasotalinja
Huhtikuu 2017

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
SMOHJ 11	**Ilmasotalinja**
Tekijä **Yliluutnantti Ville Paukku**	
Tutkielman nimi **LANGATTOMIEN VERKKOJEN SUOJAUS MAANTIETUKIKOHTAYMPÄRISTÖSSÄ**	
Oppiaine johon työ liittyy Sotatekniikka	Säilytyspaikka Maanpuolustuskorkeakoulun kirjasto
Aika Huhtikuu 2017	Tekstisivuja 60 Liitesivuja 0

TIIVISTELMÄ

Tässä tutkimuksessa perehdytään IEEE 802.11 standardin mukaisten langattomien verkkojen toimintaan ja rakenteeseen. WLAN-verkkojen kehitys on viimeisen parin kymmenen vuoden aikana ollut nopeaa ja niiden käyttö on yleistynyt niin yksityiskäytössä kuin yritysten sisällä. Tämä on tuonut kuvioihin mukaan verkkohyökkäykset, joilla pyritään pääsemään käsiksi langattomasti liikkuvaan dataan.

Tutkimuksen teoriaosassa tutustutaan tarkemmin 802.11 standardin MAC-kerrokseen ja fyysiseen kerrokseen. Lisäksi alkuun käydään läpi langattomien lähiverkkojen toimintaan liittyvää radiotekniikkaa ja antennien toimintaa. 802.11 standardin toiminnassa käydään läpi datakehysten muodostaminen ja niiden lähetys. Tämän jälkeen tutustutaan verkkoon liityttäessä tehtävään käyttäjän tunnistamiseen ja siihen liittyviin uhkiin. Teoriaosion lopussa tutustutaan langattoman verkon suojausmenetelmiin ja niihin kohdistuviin tietoturvauhkiin. Läpikäytävät suojausmenetelmät ovat WEP, WPA – TKIP, WPA2 ja VPN. Jokaiseen näistä liittyy oma käyttäjäntunnistus, datakehysten salaus ja uhkakuvat.

Päätutkimuskysymyksenä on: Ovatko langattomien verkkojen olemassa olevat suojausmenetelmät riittäviä niihin kohdistuvia uhkia vastaan maantietukikohtaympäristössä? Alakysymyksinä ovat: Millaisia ovat langattomien verkkojen suojaamiseen käytettävät menetelmät? Kuinka langattoman verkon suojauksen voi toteuttaa maantietukikohtaympäristössä?

Johtopäätöksinä voidaan todeta, että verkkojen haavoittuvuus on hyvin pitkälle kiinni siitä, millaista laitteistoa niissä käytetään. Mikäli käytössä on vanhempaa tekniikkaa, on verkkoon murtautuminen melko helppoa. Uusinta suojaustekniikkaa tukeva laitteisto antaa liikkuvalle datalle hyvän suojan ja sen salausta tuskin saadaan murrettua. Salauksessa tärkeimmässä asemassa on kuitenkin salasana. Mikäli salasana on helposti arvattavissa, voidaan vahvakin salausmenetelmä murtaa brute force -menetelmällä. Langattoman luonteensa vuoksi verkoista saadaan kaivettu aina jonkinlaisia tietoja, vaikka varsinaista salausta ei pystyttäisikään murtamaan. Maantietukikohdassa avainasemaan nousevat verkon suunnittelu ja yhteyspisteiden, sekä linkkijänteiden sijoittelu maaston suhteen. Verkko tulisi rakentaa siten, että sen salakuuntelu kauempaa olisi mahdollisimman vaikeaa. Varsinaisesta salauksen murtamisesta ja sitä kautta tapahtuvasta tietomurrosta ei tarvitse olla huolissaan, kun verkkojen salasanat pidetään riittävän monimutkaisina ja ennalta-arvaamattomina.

AVAINSANAT

WLAN, IEEE 802.11, Maantietukikohta, WEP, TKIP, WPA2, VPN, Tietoturva

LANGATTOMIEN LÄHIVERKKOJEN SUOJAUS MAANTIETUKIKOHTAYMPÄRISTÖSSÄ

LANGATTOMIEN LÄHIVERKKOJEN SUOJAUS MAANTIETUKIKOHTAYMPÄRISTÖSSÄ

1. JOHDANTO

Langattomien lähiverkkojenverkkojen kehitys alkoi 1980-luvun puolivälissä, jolloin yksittäiset valmistajat alkoivat tuoda markkinoille omia tuotteitaan. Tällöin käytössä ei ollut mitään yksittäistä standardia, vaan kaikki toimittajat kehittivät omia valmistajakohtaisia tekniikoitaan. Käyttäjä joutui siis sitoutumaan yhteen valmistajaan kerrallaan. [27]

Langattoman lähiverkon standardikehitys alkoi vuonna 1990 IEEE:n toimesta ja sen lopputuloksena syntyi ensimmäinen 802.11-standardi. Samaan aikaan Euroopassa ETSI kehitti vaihtoehtoisen HiperLAN/1 standardin, josta jatkojalostettiin HiperLAN/2, mutta se jäi 802.11 standardin varjoon. Ensimmäisen 802.11:n siirtonopeus oli vain 1-2Mbit/s, joka jäi huomattavasti langallisen Fast Ethernet -lähiverkon nopeudesta. Lisäksi varhaisessa 802.11:ssa oli runsaasti yhteensopivuus- ja taajuuskaistan käyttölupaongelmia. [27][41]

Seuraava kehitysversio, 802.11b julkaistiin vuonna 1999. Maksimibittinopeudeksi tuli 11Mbit/s ja verkko määriteltiin toimimaan vapaalla 2,4Ghz taajuuskaistalla. Tämän lisäksi radiolähetyksessä käytettiin vain suorasekvenssihajaspektritekniikkaa. Aikaisemmassa standardissa ollut FHSS-taajuushyppely ja infrapunavalo poistettiin käytöstä, jotta suurempia bittinopeuksia voitiin saavuttaa. Samana vuonna julkaistiin myös 802.11a-standardi, joka käytti 5Ghz:n taajuuksia. Sen teoreettinen maksiminopeus oli 54Mbit/s. 802.11a:n ongelmaksi muodostui se, että 5Ghz:n taajuudet olivat useissa maissa varattu muuhun käyttöön. Lisäksi siinä oli hyvin lyhyt kantama ja verrattain kallis hinta. [27]

Vuonna 2003 otettiin käyttöön 802.11g, jolla päästään 54Mbit/s saakka, mutta se käyttää 802.11a:sta poiketen vapaassa käytössä olevaa 2,4Ghz taajuutta. 802.11g:n laitteisto on täysin yhteensopivaa vanhemman 802.11b:n kanssa, joten se yleistyi käyttöön hyvin nopeasti suuremman siirtonopeutensa ansiosta. Tästä edelleen kehitettiin 802.11n, joka käyttää aiemmista standardeista poiketen useita antenneja tiedonsiirtoon. Tällä tavoin tiedonsiirtonopeus on saatu nostettua 54Mbit/s:sta jopa 600Mbit/s. 802.11n käyttää sekä 2,4Ghz:n että 5Ghz:n taajuuksia. [21][23][22][27]

Langattomat lähiverkot ovat siis yleistyneet nopeasti kaikkien käytettäväksi. Nykyään langattomia liityntäpisteitä on joka puolella ja lähes jokaisessa medialaitteessa on WLAN -ominaisuus. Langattomia lähiverkkoja käyttävät niin yksityiset ihmiset, kuin suuret yritykset ja niissä liikkuu suuria määriä dataa. Langattomissa verkoissa liikkuvasta datasta iso osa on julkista, mutta siellä liikkuu myös ihmisten henkilökohtaisia tietoja ja yritysten sisäisiä asioita, joihin ulkopuolisten ei haluta pääsevän käsiksi. Langattomuuden ongelmana on se, että verkkoon voidaan päästä käsiksi sen kantaman puitteissa mistä vaan. Verkkoja on suojattava sen vuoksi, että ulkopuoliset tahot eivät pääsisi käsiksi verkon sisällä liikkuviin tietoihin. Suojausta varten on kehitetty erilaisia menetelmiä, joita on jouduttu päivittämään ja parantelemaan niistä löydettyjen heikkouksien vuoksi. Langattomuudesta johtuen verkon sisällä liikkuvan tiedon luokittelua ja salaisuutta on myös harkittava.

Tässä työssä on aluksi tarkoitus perehtyä langattoman verkon toiminnan perusteisiin käymällä läpi IEEE 802.11-standardin toimintaa, OSI-mallia ja hieman langattomiin verkkoihin läheisesti liittyvää radiotekniikkaa. Perusteiden jälkeen esitellään langattomassa tiedonsiirrossa käytössä olevia suojausmenetelmiä, joita ovat WEP, WPA, WPA2 ja VPN. Suojausmenetelmien matemaattiseen toteutukseen ei mennä yksityiskohtaisesti. Suojausmenetelmiä käsiteltäessä perehdytään myös erilaisiin uhkiin ja hyökkäyksiin, joita on suunniteltu eri suojaustyyppejä vastaan. Näiden yhteydessä käy ilmi, miksi tiettyjä suojaustapoja ei tulisi enää käyttää. Ennen johtopäätöksiä tehdään käyttötapaustutkimus langattoman verkon käytöstä kuvitteellisessa maantietukikohtaympäristössä. Käyttäjän asemassa käyttötapaustutkimuksessa on hyökkääjä, jonka tarkoitus on toimia maantietukikohtaa vastaan. Tällä pyritään kartoittamaan sitä, millaisia uhkia siirrettävän tukikohdan sisällä oleviin verkkoihin on mahdollista kohdistaa erilaisissa tilanteissa. Johtopäätöksissä vastataan tutkimuskysymyksiin. Luvussa selviää verkon suojaamiseen käytettävät menetelmät, suojauskeinot maantietukikohtaolosuhteissa ja suojauskeinojen riittävyys.

1.1. Tutkimuskysymys ja alakysymykset

Pääkysymys:

- Ovatko langattomien lähiverkkojen olemassa olevat suojausmenetelmät riittäviä niihin kohdistuvia uhkia vastaan maantietukikohtaympäristössä?

Alakysymykset:

- Millaisia ovat langattoman verkon suojaamiseen käytettävät menetelmät?
- Kuinka langattoman verkon suojauksen voi toteuttaa maantietukikohtaympäristössä?

1.2. Tutkimusmenetelmät

Tutkimusmenetelminä tässä tutkimuksessa käytetään kirjallisuusselvitystä ja käyttötapaustutkimusta. Kirjallisuusselvityksen tarkoituksena on etsiä, analysoida ja käsitellä aiemmin tuotettua tietoa. Kirjallisuusselvitys on pohja jokaiselle tutkimukselle. Kirjallisuusselvitys on muodoltaan referaatti, muttei kopioi suoraan lähdetekstiä sanasta sanaan. Lähteinä käytetään yleensä standardeja, ohjekirjoja ja tutkimusraportteja. Lähteiden tulee myös olla ajantasaisia. Kirjallisuustutkimuksen tarkoitus on tuottaa faktatietoa, käsitemääritelmiä ja asiantuntemusta aiheesta. Käytettävät lähteet voivat olla kirjoja, karttoja, videoita, äänitallenteita, valokuvia tai sähköisiä dokumentteja. Lähteet on luokiteltava niiden aiheellisuuden ja sopivuuden perusteella. Perussääntönä voidaan pitää sitä, että alemman tason tutkimuksia on käytettävä harkiten lähdemateriaalina. Lähteitä etsittäessä on myös pidettävä mielessä lähteiden luotettavuus. Luotettavina lähteinä voidaan pitää virallisia tilastoja, tieteellisiä julkaisuja, eri alojen käsikirjoja ja empiirisiä mittaustuloksia, mikäli niiden validiudesta ja reliaabeliudesta on varmistuttu. Lähdekritiikki on olennaista lähteiden valinnassa. Lähdekritiikin voi jakaa sisäiseen ja ulkoiseen kritiikkiin. Sisäinen arvioi lähteen tekijän objektiivisuutta ja tarkoitusperiä ja ulkoinen kritiikki keskittyy ulkoisten tekijöiden, kuten lähteen tekoajan, -paikan ja alkuperäisyyden tarkasteluun. Erityisesti internet-lähteiden kohdalla on syytä olla tarkkana, sillä verkkoon voi kuka tahansa ladata mitä tahansa, joka on naamioitu näyttämään aidolta ja viralliselta, mutta onkin todellisuudessa jotain muuta. [35]

Käyttötapaustutkimuksen (use case) idea on kuvata tapahtumaa tai toimintaa tietyssä ympäristössä. Käyttötapaus esitellään käyttäjän kannalta ja sillä pyritään esittämään käyttäjän ja käyttöliittymän välistä vuorovaikutusta. Käyttötapaus on vapaamuotoinen käyttötarina, jossa käydään läpi tapahtumien kulku, toiminnan tarkoitus ja tavoitteet. Tutkimuskohteena voivat olla taustatekijät, tilanne, ympäristö, sisäiset ja ulkoiset vaikuttavat tekijät. Tässä tutkimuksena käytetään kuvitteellista maantietukikohtaa ja siellä sijaitsevia langattomia verkkoja kohteena. Käyttäjänä toimii verkkoihin uhkan kohdistava taho. Ideana on käsitellä sitä, millaisia uhkia tällaiseen verkkoon voidaan kohdistaa ja voidaanko niiltä suojautua. Tilanteita kuvataan kolme: rauhan aika, kiristynyt tilanne ja sotatila. Pyrin jokaisessa tilanteessa pohtimaan hyökkääjän toimintaan vaikuttavia tekijöitä ja sitä, mitä hyökkääjän kannattaa ja ei kannata tehdä. Lopputulemana tästä on se, kuinka maantietukikohdassa tulisi suhtautua mahdolliseen verkkouhkaan eri tilanteissa. [26]

1.3. Tärkeimmät lähteet ja lähdekritiikki

Lähdekirjallisuutena on käytössä langattomien verkkojen perusteisiin ja suojaukseen keskittyvää kirjallisuutta, IEEE:n 802.11 standardeja ja niitä käsitteleviä raportteja, sekä langattoman verkon suojaukseen perehtyviä tutkimuksia ja artikkeleita. Lisäksi uhkaa käsiteltäessä käytän langattoman verkon murtamisesta kertovia teoksia kuten Hacking Exposed. Aihealueesta löytyy hyvin runsaasti ajankohtaista materiaalia verkosta. Internet-lähteiden kanssa tarkoitus on pyrkiä varmistamaan tiedon oikeellisuus useammasta kuin yhdestä lähteestä. Internetlähteiden kanssa pyrkimys on käyttää PDF-muotoon tallennettuja artikkeleita ja tutkimuksia. Niiden oikeellisuus on helpommin arvioitavissa, kuin yksittäisten nettisivujen kirjoitukset. IEEE:n standardeja voi lähtökohtaisesti pitää luotettavina, kuin myös kirjallisia teoksia. Nykypäivänä kirjallisena teoksena voidaan myös pitää digitaaliseen muotoon tallennettua kirjaa, joka usein miten on PDF -muodossa.

2. LANGATTOMAN LÄHIVERKON PERUSTEET

2.1. Langattoman lähiverkon radiotekniikka

2.1.1 Radioaaltojen ominaisuuksia

Kuten kaikki muutkin langattomasti toimivat laitteet, myös langaton verkko käyttää sähkömagneettisen spektrin taajuusalueita toimiakseen. Radioaallot toimivat taajuuksilla, jotka ulottuvat alhaisista LF taajuuksista (30kHz) ultrakorkeisiin UHF taajuuksiin (3GHz). Tätä taajuusaluetta käytetään pääosin radio- ja tv-lähetyksiin. Mitä matalampi taajuus on, sitä pidempi sen kantama on. Radio- ja mikroaaltoalueen teknistä käyttöä on rajoitettu runsaasti ja sen käyttö vaatii lähes poikkeuksetta kansallisen viranomaisen luvan. Suomessa lupia hallinnoi viestintävirasto. UHF alueella on yksi vapaasti käytettävä taajuuskaista 900MHz:ssä. Radioaaltoja korkeammilla taajuuksilla olevia mikroaaltoja käytetään yleensä tietoliikenteessä ja tutkissa. Mikroaallot ovat 1GHz-300GHz väliin sähkömagneettisessa spektrissä jäävä taajuusalue. Mikroaaltoalueella on kaksi vapaasti käytettävää taajuusaluetta. Toinen on 80Mhz leveä kaista 2,4GHz:n yläpuolella ja toinen on kolme 100MHz:n kaistaa hieman 5GHz:n yläpuolella. Näitä kahta kaistaa käytetään myös langattomien lähiverkkojen tiedonsiirrossa. Samoilla taajuuksilla toimii myös monia muita teknisiä laitteita, jotka voivat vaikuttaa langattoman verkon toiminaan ja päinvastoin. [27]

Radio- ja mikroaaltoja voidaan kuvata erilaisin parametrein:

- Taajuudella tai aallonpituudella. Ne ovat kääntäen verrannollisia toisiinsa. Eli mitä korkeampi taajuus, sitä pienempi aallonpituus 2,4GHz:n taajuusalueella aallonpituus on 12,5 cm. [27]

- Vaihekulmalla, joka tulee esiin useamman aallon yhteenlaskussa. Mikäli saman lähettimen aallot etenevät vastaanottimelle eri reittejä, ne saapuvat perille eri vaiheessa. 180 asteen vaihe-erossa olevat aallot kumoavat toisensa. Vastaavasti samassa vaiheessa olevat aallot vahvistavat toisiaan. [27]

- Teholla. Lähetetty signaali vaimenee väliaineessa, josta johtuu, että lähetetty signaali on suuritehoisempi kuin vastaanotettu. [27]

- Polarisaatio määräytyy antennin kulmasta ja ominaisuuksista. Langattomissa lähiverkoissa käytetään yleensä pystypolarisaatiota, joka toteutetaan antennin sijoittelulla. [27]

Luotettavaa tiedonsiirtoyhteyttä varten pitää vastaanotetun signaalin taso olla riittävä suhteessa häiriöihin. Radiolaitteiden lähetystehoa kuitenkin rajoitetaan tehonkulutuksen ja määräysien vuoksi. Tiedonsiirrossa tärkein kriteeri on riittävä vastaanottoteho. Vastaanottoteho riippuu lähettimen tehosta ja signaalin vaimenemisesta yhteyspisteen ja käyttölaitteen välillä. Radiolähetteen syöttö- ja lähetystehoa mitataan watteina ja sen osina. Väliaineen vaimennuksen vaikutus on logaritminen. Tämän vuoksi tehotasoja käsitellään logaritmisella desibeliasteikolla. [27]

Langattoman verkon yhteyspisteissä ja -sovittimissa 802.11b-laitteiden lähetysteho ei saa ylittää 100mW:ia. Yhteyspisteen lähetystehoa laskettaessa on otettava huomioon antennin vahvistus ja antennikaapelin vaimennus. Vaimennus voidaan laskea negatiivisena vahvistuksena. [27]

Myös polarisaatio vaikuttaa langattoman verkon toimintaan. Polarisaatio riippuu antennin asennosta, joten vastaanotto ja lähetysantenni kannattaa sijoittaa samaan kulmaan maanpinnan suhteen. Mikäli kantaman alueella on useampia suunta-antennein toteutettua langattoman verkon yhteyspistettä, ne häiritsevät toisiaan. Häiriöt voidaan kuitenkin minimoida käyttämällä eri antenneille eri polarisaatiota. [27]

2.1.2 Radioaaltojen eteneminen

Radioaaltojen etenemiseen vaikuttaa kaikissa ympäristöissä, paitsi tyhjiössä väliaine ja esteet. Radioaaltojen kulkuun vaikuttavat seuraavat perusilmiöt:

- Vaimeneminen pienentää amplitudia ja tehoa. Tehon pieneneminen riippuu taajuudesta ja väliaineen ominaisuuksista. Tehon pienenemiseen vaikuttaa myös väliaineessa kuljettu matka. Kaikilla kappaleilla on taajuuskohtainen vaimennusarvo, joka ilmaistaan desibeleissä metriä kohti. Mitä suurempi taajuus, sitä enemmän se vaimenee väliaineessa. [15][27]

- Useimmiten sisätiloissa käytettäviin WLAN-lähetteisiin vaikuttaa myös heijastuminen. Sitä tapahtuu, kun säteily osuu kahden aineen rajapintaan oikeassa kulmassa. Langattoman verkon tapauksessa toinen aineista on useimmiten ilma. Heijastumisen määrä riippuu säteilyn tulokulmasta. Mitä suurempi kulma, sitä vähemmän säteilyä heijastuu. Väliaineen pinnanmuodot vaikuttavat heijastumisen suuntaan. Karkeasta pinnasta heijastumista tapahtuu useampiin suuntiin. [15][27]

- Heijastumisen lisäksi säteilyn osuessa rajapintaan tapahtuu taittumista. Osa säteilystä tunkeutuu toiseen väliaineeseen ja muuttaa samalla kulmaansa rajapinnan taitekertoimen mukaan. [15][27]

- Muita säteilyyn vaikuttavia tekijöitä on taipuminen ja sironta, mutta ne eivät juurikaan vaikuta langattomien lähiverkkojen toimintaan. Niillä on vaikutusta lähinnä matalien taajuuksien pitkiä matkoja kulkeviin radioaaltoihin. [15][27]

Langattomien verkkojen käyttöön vaikuttavat siis kolme ensin mainittua ominaisuutta. WLAN-lähetin voi olla eri huoneessa, kuin sovitin, jolloin yhteyspisteen lähettämä säteily kulkee seinien läpi samalla heijastuen niistä. Tällöin on kyseessä monitie eteneminen. Monitie-etenemisessä sama lähete tulee vastaanottimelle useassa eri vaiheessa. Mikäli vaihe-ero on lähellä 180 astetta, on summa-aalto lähellä nollaa, jolloin tapahtuu lähetyksen häipyminen. Langattomissa verkoissa käytetään hajaspektri- ja kaksiantennitekniikoita, joilla pyritään kompensoimaan monitie-etenemisen aiheuttamaa häipymistä. Tämän vuoksi sisätiloissa yli viiden metrin etäisyyksillä vaimeneminen tapahtuu hyvin monimutkaisen matemaattisen kaavan mukaan. Lisäksi jos välissä on ovia, seiniä, ikkunoita ja lattioita, monimutkaistuu laskukaava entisestään ja siitä tulee sen lisäksi niin epätarkka, että yhteyspisteen kantama täytyy mitata käytännön toimenpitein. [27]

2.1.3 Antennit

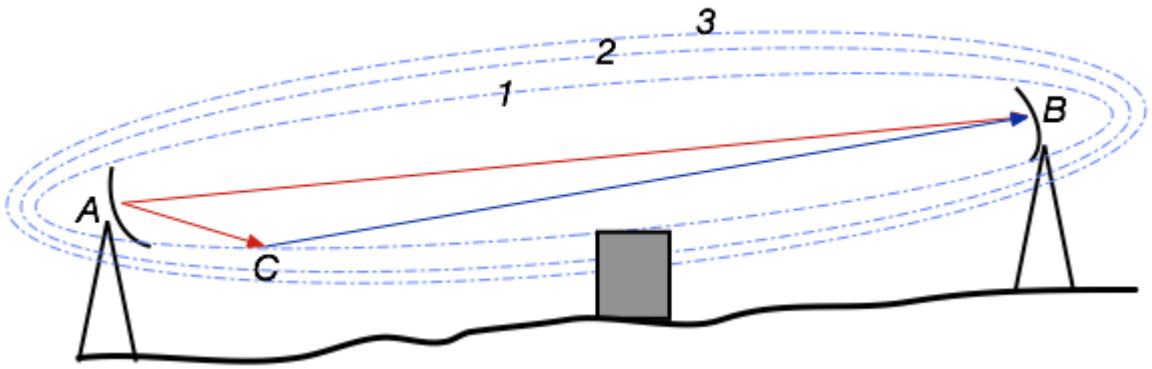
Lähetysantenni muuttaa sähkötehon sähkömagneettiseksi säteilyksi ja vastaanotinantenni muuttaa säteilyn sähköiseksi signaaliksi. Langattomissa lähiverkoissa käytettäviä antenneja käytetään samaan aikaan sekä lähetykseen, että vastaanottoon. Pienten lähiverkkojen antennit ovat yleensä ympärisäteileviä dipoli-antenneja. Täysin ympärisäteilevä pistemäinen isotrooppinen antenni säteilee tehoa samalla tavalla kaikkiin suuntiin. Käytännössä minkään ympärisäteilevän antennin säteilykuvio kuitenkaan ei ole symmetrinen, vaan niiden säteilyteho vaihtelee suunnasta riippuen. Mikäli halutaan tarkoituksella epäsymmetrinen säteilykuvio, käytetään suunta-antennia. Ne vahvistavat sähkömagneettisia aaltoja haluttuun suuntaan verrattuna ympärisäteilevään antenniin. Suunta-antennin antennivahvistus lasketaan yleensä pistemäiseen antenniin verrattuna ja se ilmoitetaan dBi-asteikolla eli desibeleinä isotrooppiseen antenniin verrattuna. Ilmoitettu vahvistus pätee vain korkean vahvistuksen suuntaan. [15][27]

Langattomien verkkojen tapauksessa käytössä olevan antennin tyyppi määräytyy monesti käyttötavan mukaan. Tukiasemissa on monesti ympärisäteilevät antennit, joilla pyritään mahdollisimman suureen kattavuuteen tai tietylle sektorille säteilevät antennit, joilla on tarkoitus luoda kuuluvuus juuri halutulle pienemmälle alueelle. Mikäli halutaan luoda yhteys kahden

yksittäisen pisteen välille, käytetään yleensä suuntaavia antenneja. Tällaisia antenneja ovat yagi- ja lautasantennit. Yagi antennin rakenne koostuu useista suorista elementeistä, jotka ovat noin puolen aallonpituuden mittaisia. Aktiivisena elementtinä on puolen aallonpituuden mittainen dipoliantenni, jonka molemmin puolin 0,2-0,5 aallonpituuden etäisyydelle on kiinnitetty vaijerit tai tangot, jotka toimivat ohjaajina ja heijastimina. Dipoliantennin takana oleva heijastin on hieman yli puolen aallonpituuden mittainen. Normaalisti yagi antennissa on yksi heijastin- ja useampi ohjain-elementti. Yagi:n säteily suuntautuu aktiiviselta elementiltä suoraan eteenpäin ohjaajien suuntaan ja sen vastaanotto on myös herkimmillään edestäpäin. Mitä enemmän ohjaajia antennissa on, sitä suurempi on sen antennivahvistus. Linkkijänteenä käytettävissä Yagi antenneissa on usein 10-20dBi:n antennivahvistus ja 10-20 asteen keilanleveys. [8][27]

Toinen linkkijänteiden välillä käytetty antennimalli on lautasantenni. Lautasantennilla saadaan aikaan halutun kokoinen antennivahvistus ja suuntaus. Se muuntaa pistemäisestä lähteestä tulevan säteilyn tasaiseksi aalloksi. Vastaavasti vastaanotettaessa signaalia, antenni kerää säteilyn isolta alueelta ja heijastaa sen yhteen pisteeseen. Lautasen koko määrittää antennivahvistuksen maksimin lähetettävällä taajuudella ja kaistanleveydellä. Lautasen halkaisijan kaksinkertaistuessa vahvistus nelinkertaistuu. [8][27]

Muodostettaessa pitkiä kahden pisteen välisiä yhteyksiä, täytyy antennien välillä olla näköyhteys (LOS). Radioaalto taipuu matkan varrella jonkin verran, joka saa aikaan sen, että radiohorisontti on hieman geometrista horisonttia kauempana. Kun yhteys toimii näköyhteyden sisäpuolella, vaimentavat ensimmäisen Fresnellin vyöhykkeen sisällä olevat esteet signaalia. Toisin sanoen, jotta yhteys toimisi mahdollisimman hyvin, tulisi tämän vyöhykkeen olla tyhjä. Fresnellin vyöhykkeet ovat ellipsejä, joilla lähettimestä lähteneet aallot ovat edenneet puoli aallonpituutta tai sitä enemmän, kuin suoraa lähettimeltä vastaanottimelle kulkevat aallot. Kehät muodostuvat siten, että ensimmäinen kehä on puoli aallonpituutta edellä, toinen yhden aallonpituuden, kolmas puolitoista aallonpituutta ja niin edelleen. Ensimmäisen vyöhykkeen sisältä heijastuvat säteet, jotka saapuvat vastaanottimelle vahvistavat suoraan kulkevaa aaltoa. Kun taas ensimmäisen vyöhykkeen ulkopuolelta tulevat säteet saattavat joko vahvistaa tai vaimentaa suoraan kulkevaa aaltoa riippuen kuljetusta matkasta. Suurin osa kokonaisenergiasta liikkuu ensimmäisen kehän sisäpuolella. [15]



Kuva 1: Fresnelin vyöhykkeet [17]

2.2. OSI -malli

Jotta langattoman verkon toimintaan voidaan mennä syvällisemmin, täytyy ensin käydä läpi OSI -malli, joka kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. idea on, että kukin kerroksista käyttää alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs.

Kuva 2: OSI-mallin havainnekuva. [30]

2.2.1 Fyysinen kerros

Fyysinen kerros on OSI-mallin alin kerros. Se käsittää raa'an datan lähettämisen ja vastaanottamisen fyysisten yhteyksien kautta. Tämä käsittää elektroniset, optiset ja mekaaniset osat, joiden kautta signaalit kulkevat ylemmille kerroksille. Fyysinen kerros määrittää lähtevien ja vastaanotettavien signaalien 1:t ja 0:t. Se päättelee, mikä vaihe signaalista on 1 ja mikä 0. Se myös päättelee signaaleista sen, milloin vastaanotettavaa dataa alkaa tulla. Fyysinen kerros käsittää myös tiedon siitä millaista rautaa on käytössä ja määrittelee jokaisen yksittäisen pinnin käytön. Kerros määrittää myös sen, kuinka paljon virtaa tai desibelejä jokin lähetys vaatii ja mitä kautta se tehdään. Käytännössä fyysinen kerros siis käsittää hardware puolen. Yksinkertainen esimerkki fyysisen kerroksen laitteesta on verkko-hubi, jonka tehtävänä on ainoastaan jakaa jokin yhteys useampaan paikkaan. [29][30]

2.2.2 Siirtokerros

Siirtokerros tarjoaa datan virheettömän siirron solmukohdasta toiselle, fyysisen kerroksen yli, joka mahdollistaa ylempien kerrosten datan virheettömyyden. Siirtokerros luo ja purkaa yhteyksiä solmukohtien (node) välillä ja jaksottaa datan lähetystä ja vastaanottoa näissä yhteyksissä. Siirtokerros olettaa, että jokainen lähetetty datapaketti kuitataan vastaanotetuksi, jotta virheiltä vältytään. Mikäli kuittausta ei tule, lähettää siirtokerros saman paketin uudestaan, kunnes se kuitataan vastaanotetuksi. Siirtokerros luo ja havaitsee pakettien rajoja ja tarkistaa pakettien eheyttä. Siirtokerros määrittelee myös sitä, milloin jollain tietyllä solmulla (node) on oikeus käyttää fyysistä kerrosta. [29][30]

2.2.3 Verkkokerros

Verkkokerros kontrolloi datan kulkua aliverkossa. Se päättää mitä fyysistä reittiä datan tulisi kulkea erilaiset vaikuttavat tekijät huomioiden. Verkkokerros reitittää datapaketteja verkossa. Se jarruttaa reitittimille lähetettävien datapakettien määrää, kun se havaitsee niiden puskurien täyttyvän. Verkkokerros voi myös pilkkoa lähetettäviä datapaketteja pienemmiksi reitittimien ominaisuuksien mukaan ja koota ne takaisin yhtenäisiksi vastaanottopäässä. Verkkokerros myös muuttaa loogiset osoitteet ja nimet fyysisiksi osoitteiksi. [29][30]

2.2.4 Kuljetuskerros

Kuljetuskerros vastaa lähetettävien viestien virheettömyydestä ja vaiheistuksesta. Se myös vastaa siitä, ettei viesteihin tule häviöitä tai, että ne eivät monistu. Kuljetuskerros huolehtii, ettei ylempien kerrosten protokollien tarvitse huolehtia datan kulusta. Kuljetusprotokollan koko ja monimutkaisuus riippuvat hyvin paljon verkkokerroksesta. Mikäli verkkokerros on epäluotettava, tulisi kuljetusprotokollassa olla virheiden tunnistus- ja korjausominaisuuksia. Kuljetuskerros kykenee vastaanottamaan melko suuriakin viestejä, mutta joutuu pilkkomaan niitä pienemmiksi kokonaisuuksiksi verkkokerrosta varten. Vastaanottopäässä kuljetuskerros jälleen kokoaa pilkotun viestin yhtenäiseksi paketiksi. Lähetyspään kuljetuskerros merkitsee pakettien alut ja loput, jotta vastaanottopää tunnistaa viestien rajat ja osaa koota ne oikein. Kuljetuskerros toimii siis kuten posti. Se vastaa pakettien lähettämisestä oikeisiin osoitteisiin. [29][30]

2.2.5 Istuntokerros

Istuntokerros luo ja sulkee yhteyksiä eri työasemien välille. Näitä yhteyksiä kutsutaan istunnoiksi. Istunnot mahdollistavat työasemien välisen tiedon välityksen, tunnistuksen, kirjautumisen ja turvallisuuden. Erimallisia yhteyksiä ovat: kaksisuuntainen, vuorosuuntainen ja yksisuuntainen yhteys. Kaksisuuntaisessa yhteydessä viestejä voidaan lähettää molempiin suuntiin samanaikaisesti. Vuorosuuntaisessa yhteydessä lähetettävät viestit kulkevat vuorotellen eri suuntiin. Vastaanottajan tulee siis vastaanottaa koko viesti, ennen kuin se voi lähettää omansa takaisin. Yksisuuntaisessa yhteydessä viestit kulkevat vain yhteen suuntaan. [29][30]

2.2.6 Esitystapakerros

Esitystapakerros kääntää viestit sovelluskerrokselle ymmärrettävään muotoon ja päinvastoin. Esityskerros myös pakkaa ja salaa lähetettäviä viestejä ja vastaavasti purkaa vastaanotettuja viestejä. [29][30]

2.2.7 Sovelluskerros

Sovelluskerroksen kautta käyttäjä ja sovelluksien prosessit pääsevät käsiksi verkkoon. Sovelluskerroksen toimintaan kuuluvat kaikki perus toiminnot, joita käyttäjä voi verkon yli käyttää. Näihin kuuluvat muun muassa sähköposti, etäyhteydet eri laitteisiin ja tiedostojen jakaminen. [29][30]

2.3. IEEE:n 802.11 standardit

IEEE:n 802.11-standardit kattavat OSI-mallin kaksi alinta kerrosta: siirtokerroksen ja fyysisen kerroksen. 802.11 standardit käyttävät LLC-protokollaa ja -kehystä. LLC kehystää verkkokerrokselta saaman paketin ja tarjoaa yhteiset rajapinnat verkkokerroksen protokollille ja eri alue- ja lähiverkkotekniikoille. Yleisimmät käytössä olevat protokollat, joita käytetään sovelluskerrokselta verkkokerrokselle, on TCP/IP-pinon protokollat. Niiden mukaan verkkokerroksella reititetään IP-paketteja, jotka sisältävät TCP-segmentin tai UDP-tietosähkeen, johon sovelluskerroksen sanoma sisältyy. [27]

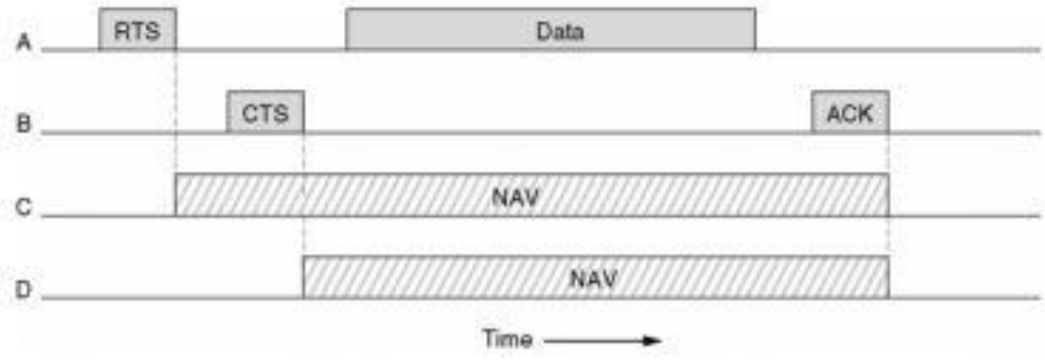
Siirtokerroksen ja verkkokerroksen väliset palvelut ovat yleisimmin kuittaamattomia ja yhteydettömiä datapalveluja, mutta käytettävissä ovat myös kuittaava yhteydellinen ja kuittaava yhteydetön palvelu. Toteutuksessa IP-paketti kehystetään LLC kehykseen, jonka otsikossa on protokollatunnukset ja ohjauskenttä. IP:lle voidaan käyttää joko LLC:n protokolla tunnusta SAP:a tai SNAP-kehystä. Yleisimmin käytössä on SNAP, joka tarjoaa vain yhteydettömän kuittaamattoman palvelun. Tästä syystä kaikki kehykset ovat numeroimattomia infokehyksiä. Tällöin IP-protokolla tunnistetaan Ethernet-kehyksen mukaisella Ethertype-tunnuksella. [27]

LLC/SNAP-toteutuksen alapuolella on 802.11 MAC-alikerros, jonka vuoronvaraus määrittää. MAC-alikerros tarjoaa asynkronisia datapalveluja kellottomalle kehysten lähetykselle, WEP-protokollan tietoturvapalveluja, sekä tietosähkeiden uudelleenjärjestyspalveluja. Uudelleenjärjestystä tarvitaan, koska radiotiet ovat hyvin häiriöllisiä. Virheettömyyden varmistamiseksi ja siirron helpottamiseksi LLC-kehykset pilkotaan pienemmiksi osiksi. MAC-alikerros kehystää LLC-kehyksen MAC-tietosähkeeksi (MPDU), jonka otsikosta löytyy kehyksen ohjaus, vuoron varauksen kesto, uudelleenjärjestelyn sekvenssitieto, osoitteet ja virheettömyyden varmistava tarkistussumma. MAC-kerros määrittää kehysten väliset ajat ja CSMA/CA-vuoronvarauksen. Tiedonsiirronsiirron luotettavuus pyritään varmistamaan datakehysten kuittauksilla ja datan puskuroinnilla. [27]

Fyysisessä kerroksessa on kaksi alikerrosta. Ylempänä on konvergenssiprotokolla, joka sovittaa bittinopeudet ja fyysiset siirtotiet yhtenäiseksi palveluksi. Sen tärkein toiminto on nimenomaan lähettäjän ja vastaanottajan bittinopeuksien sovittaminen yhteen. Se määrittää molemmilta suurimman mahdollisen bittinopeuden ja sovittaa sen yhteen. 802.11b-verkoissa tahdistusmerkki lähetetään 1Mbit/s, otsikko 2Mbit/s ja itse datakenttä suuremmilla nopeuksilla. Alin kerros on fyysinen mediasta riippuva kerros, joka määrittelee modulaation, kanavointitavan ja hajaspektritekniikan. Eri bittinopeuksille on määritetty niille ominaiset modulaatiomenetelmät. [27]

2.3.1 MAC kerros

Langattomissa lähiverkoissa on käytössä CSMA/CA vuoronvarausmenetelmä. Se on yhteneväinen Ethernetin CSMA/CD-kilpavarauksen kanssa, sillä erotuksella, että törmäysten havaitseminen on korvattu niiden välttämisellä. Tämä siksi, että kaksi toisistaan kaukana olevaa WLAN-päätelaitetta kuulevat yhteyspisteen lähetyksen, mutta eivät toisiaan signaalin vaimenemisen vuoksi. CSMA/CA mahdollistaa virtuaalisen kantoaallon kuuntelun WLAN-yhteyspisteen kanssa. Tässä tapauksessa yhteyspiste kontrolloi siihen yhteydessä olevia pääteasemia ja myöntää niille lähetysajat yksi kerrallaan. Päätelaite pyytää lähetyslupaa RTS-sanomalla, johon yhteyspiste vastaa CTS sanomalla, kun yhteys on vapaa. Päätelaite lähettää tämän jälkeen datan yhdessä tai useammassa kehyksessä, joiden vastaanotto kuitataan erikseen. [27]



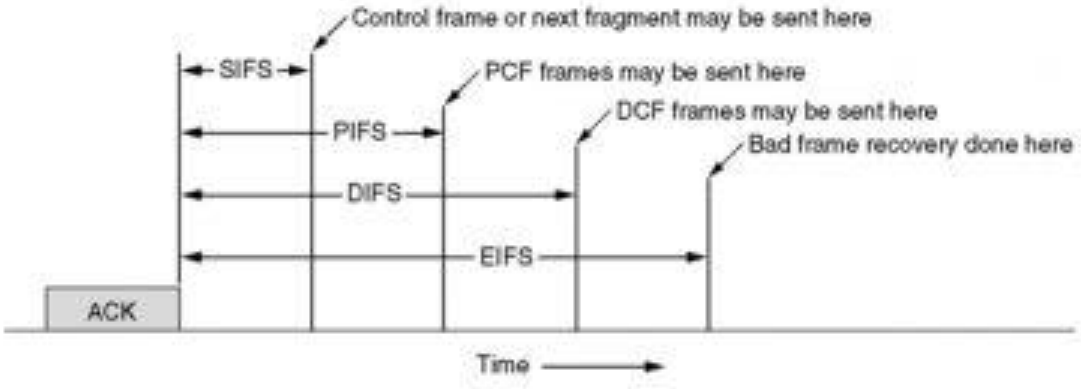
Kuva 3: Virtuaalisen kantoaallon kuuntelu [16]

Fyysinen kantoaallon kuuntelu taas tarkoittaa sitä, että pääteasema kuuntelee kanavaa ja varmistaa, että se on vapaa, ennen kuin alkaa lähettää dataa. Tällöin kehykset eivät seuraa toinen toistaan, vaan niiden välissä on jokin seuraavista ajoista:

- SIFS-aika (Short Inter Frame Space). SIFS:a käytetään toisiinsa liittyvien kehysten, kuten datakehyksen ja kuittauksen välillä. Fyysinen standardi määrittelee SIFS-ajan pituuden. [27]

- Kilpailuttoman toiminnan PIFS-aika (PCF Inter Frame Space). PIFS:ssa kehykset, joilla on etuoikeus, voidaan lähettää muuta liikennettä ennen. Tällöin lähettävän aseman pitää odottaa kanavan vapautumista kahden SIFS-ajan verran. [27]

- Normaalin Best Effort -liikenteen DIFS-aika (DCF Inter Frame Space), joka on pitempi, kuin edellinen PIFS-aika. Asema odottaa satunnaisen asemakohtaisen odotusajan (back-off time) ennen lähetystä. Odotusaika on perusaika kerrottuna satunnaisluvulla. Aluksi satunnaisluku on väliltä 0-31, mutta mikäli kaksi asemaa saa tismalleen saman satunnaisluvun ja tapahtuu törmäys, tuplaantuu satunnaislukujen väli jokaisen törmäyksen jälkeen 1023:een saakka. Jokaisen törmäyksen jälkeen asemille annetaan siis uusi satunnaisluku isommasta lukujen joukosta. [27]



Kuva 4: Fyysisen kantoaallon kuuntelu [16]

Kun asema haluaa lähettää, se sijoittaa MPDU-kehyksen kestokenttään varausajan, jonka se olettaa tarvitsevansa kehyksen lähettämiseen ja kuittaamiseen. Asema varaa verkon itselleen verkonvarausvektorilla, jonka kaikki yhteyspisteeseen yhteydessä olevat asemat kuulevat. Varausaikaa voidaan tarkentaa seuraavissa kehyksissä. Kehystenvälisen ajan laskenta ja kilpailu alkavat vasta varauksen päättymisen jälkeen, vaikka lähetys loppuisikin ennen sille asetetun varausajan päättymistä. [27]

MPDU-kehys koostuu seuraavista kentistä:

- Kehyksen ohjaus, joka sisältää 802.11-protokollan versiotiedon, sanoman tyypin ja alityypin, kehyksen kulkusuunnan, seuraako kehystä lisää sirpaleita, uudelleenlähetystiedon, tiedon salauksesta, tehonsäästötiedot ja tiedon kehysten järjestyksen seurannasta. [27]

- Kaksitavuinen kesto/tunnus, johon kuuluu vuoronvarausvektorin arvo tai AID-arvo. Varausaika ilmoitetaan verkonvarausvektorissa mikrosekunteina ja etuoikeutetulle lii-

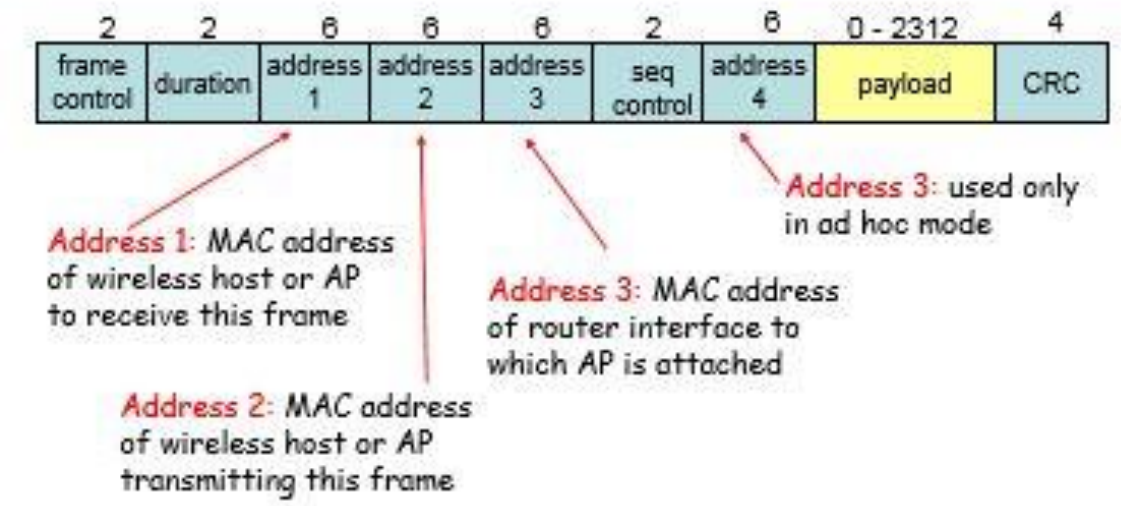
kenteelle varausaikana käytetään sopivan suurta arvoa. Asemat päivittävät omat NAV-arvonsa luettuaan kaikkien kehysten varausvektorien arvot. [27]

- Kolme tai neljä osoitetta, joista käy ilmi radiotie ja lähettäjän, sekä vastaanottajan osoite. Yleisin tapa osoitteiden järjestykselle on seuraava: ensimmäinen osoite on radiovastaanottajan osoite, toinen radiolähteen osoite, kolmatta osoitetta vastaanottaja käyttää suodatukseen. Neljäs osoite on käytössä siltaverkoissa, joissa sillä ilmaistaan varsinaisen lähettäjän MAC-osoite. Neljäs osoite voidaan jättää pois kehyksestä, kun sitä ei tarvita. Kaikki osoitekentät muodostuvat kuudesta tavusta. [27]

- Sekvenssikontrollin numeroinnilla tunnistetaan pilkotun LLC/SNAP-kehyksen osat. Tämän avulla alkuperäinen data saadaan koottua siitä huolimatta, että kehyksen osat saapuisivat vastaanottajalle eri järjestyksessä puskuroinnin tai uudelleenlähetyksen vuoksi. [27]

- Datakenttä sisältää LLC-kehyksen tai sen osan. Datakentän maksimipituus on 2312 tavua, joka on Ethernet-kehyksen datakentän 1500 tavun maksimikokoa suurempi. LLC-kehykset voidaan pilkkoa pienemmiksi osiksi luotettavuussyistä. [27]

- Tarkistussummalla varmistetaan kehyksen virheettömyys. Tarkistussumma lasketaan polynomijakolaskun jakojäännöksenä. Generointipolynomina käytetään samaa polynomia kuin Ethernet-verkoissa. [27]

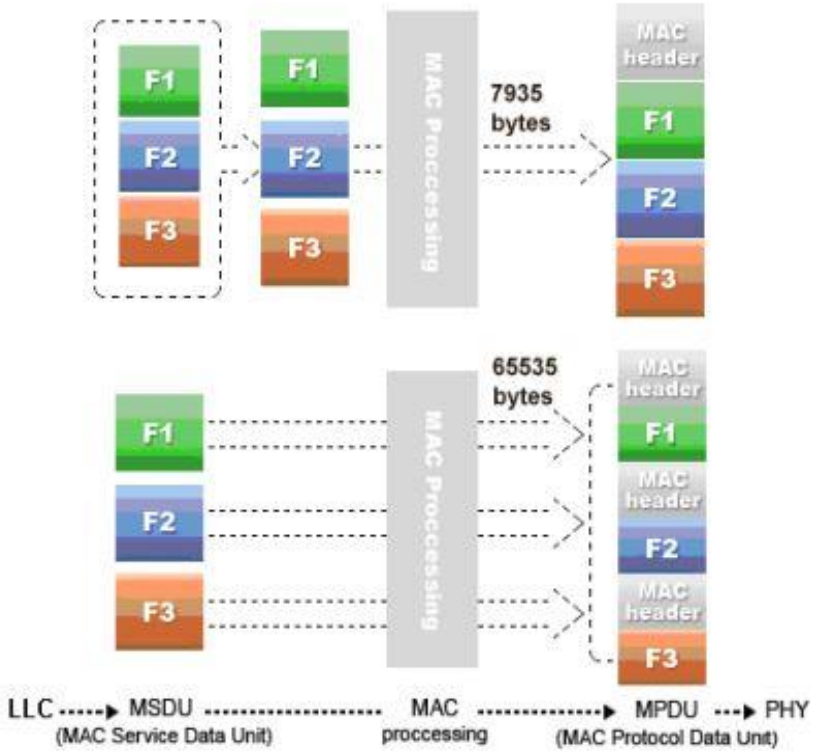


Kuva 5: MPDU-kehyksen rakenne [16]

Kaikki muut osat kehyksestä paitsi itse datakenttä ovat otsaketietoja, joiden avulla kehys saadaan oikeaan paikkaan virheettömänä ja oikein koottuna. Datakenttä on kehyksen varsinainen hyötykuorma. Kehyksiä lähetetään tiedonsiirrossa luonnollisesti todella suuria määriä, jolloin myös otsaketietojen määrä kokonaistavumäärästä alkaa olla merkittävä. Tämän vuoksi on kehitetty A-MPDU ja A-MSDU-kehykset, joita uudempi 802.11n standardi osaa käyttää. Ideana on yhdistää useampia pienempiä MSDU tai MPDU-kehyksiä yhdeksi isommaksi kehykseksi. Tämä vähentää otsaketietojen määrää merkittävästi. Tämän lisäksi myös kehysten vastaanottokuittauksia voidaan tehdä kootusti, jolloin kuittaukset tulevat kaikki samassa Block Ack-viestissä. Vanhempi 802.11g pystyy lähettämään 2304 tavua datakentässä jokaisen otsakkeen alla. A-MSDU nostaa määrän 7935:n ja A-MPDU edelleen 65535 tavuun. [1][4]

A-MSDU kehykseen voidaan liittää useampi MSDU-kehys vain, jos niillä on otsakkeissa samat osoitetiedot. Kehysten prioriteetti tulee myös olla sama. Jos salaus on päällä, kaikki MSDU kehykset kryptataan yhdeksi paketiksi A-MSDU-kehykseen. A-MPDU-kehyksessä jokainen MPDU-kehys kryptataan erikseen. Jokaisella MPDU-kehyksellä tulee olla sama vastaanottimen osoite. A-MPDU vaatii käyttöön myös kootun vastaanotto kuittauksen Block Ack:n. [1][13]

Koska kaikki 802.11 protokollaversiot ovat yhteensopivia keskenään, määrittää vanhempaa protokollaa käyttävä laitteisto yhteyden nopeuden. Kehysten yhdistäminen on käytössä vain 802.11n-protokollasta ylöspäin, joten vanhempien laitteiden kanssa joudutaan edelleen käyttämään normaaleja MPDU ja MSDU-kehyksiä. Se rajoittaa verkon nopeuden käytännössä 54Mbit/s. [1][4]



Kuva 6: A-MSDU ja A-MPDU-kehykset [4]

2.3.2 Fyysinen kerros

Kuten OSI-mallista nähdään, fyysistä kerrosta käytetään konkreettisesti datan siirtoon. Langattoman lähiverkon tapauksessa se tarkoittaa datan saattamista muotoon, jossa se voidaan lähettää radiosignaalina antennilta toiselle. 802.11 protokollat käyttävät versiosta riippuen eri taajuuskaistaa, kaistanleveyttä ja modulaatiota signaalin lähettämiseen. [27][39]

IEEE 802.11 PHY Standards						
Release Date	Standard	Frequency Band (GHz)	Bandwidth (MHz)	Modulation	Advanced Antenna Technologies	Maximum Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	N/A	11 Mbits/s
1999	802.11a	5 GHz	20 MHz	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	N/A	542 Mbits/s
2009	802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	MIMO, up to 4 spatial streams	600 Mbits/s
2013	802.11ac	5 GHz	40 MHz, 80 MHz, 160 MHz	OFDM	MIMO, MU-MIMO, up to 8 spatial streams	6.93 Gbits/s

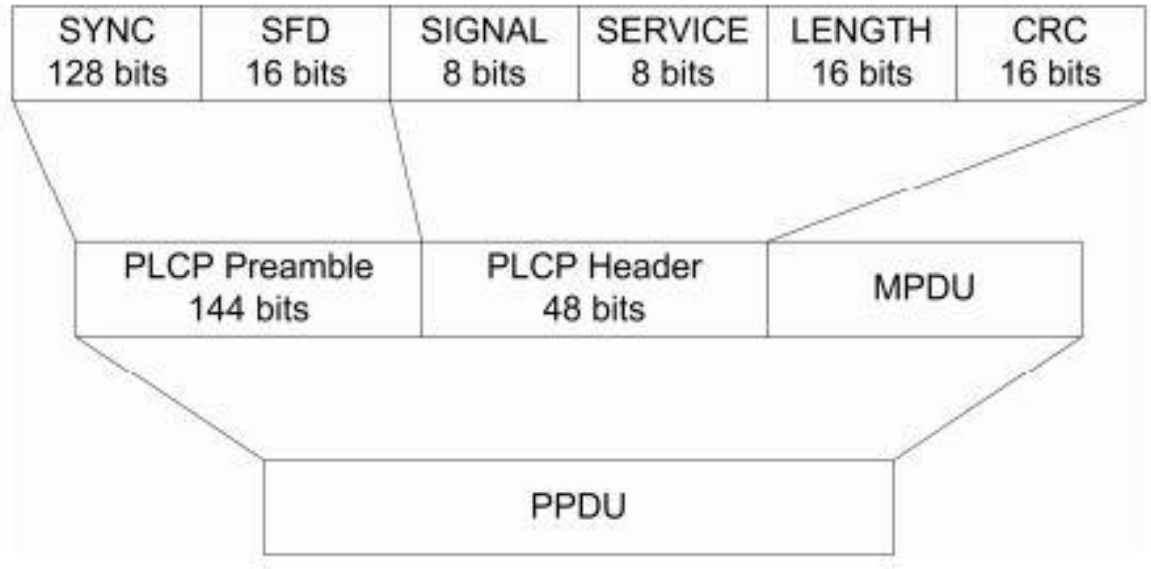
Kuva 6: 802.11 fyysiset standardit [39]

802.11b käyttää ainoastaan 2,4GHz:n taajuuskaistaa ja sen bittinopeudet ovat 1, 2, 5,5 ja 11Mbit/s. Se käyttää lähetyksessä suorasekvenssihajaspektritekniikkaa. 802.11b laitteet ovat nykyisin vanhoja, mutta niitä saattaa olla vielä käytössä, sillä ne ovat edelleen yhteensopivia uudempien laitteiden kanssa. [27]

Fyysinen kerros on jaettu kahdeksi alikerrokseksi, PLCP-konvergenssikerrokseksi ja PMD-kerrokseksi. Konvergenssikerros lisää MPDU-kehyksiin oman PPDU-otsikon, jonka tehtävä on varmistaa siirtonopeuksien sovitus. 802.11b:n konvergenssikerroksessa on olemassa pitkä ja lyhyt PPDU-kehys. Niissä molemmissa on alkumerkki, otsikko ja datakenttä. Datakenttä koostuu MPDU-kehyksestä. Aluksi lähetetään alkumerkki 1Mbit/s nopeudella. Tällöin käytetään DBPSK-modulaatiota ja siinä on kaksi kenttää: synkronointimerkki (sync) ja kehyksen alkulippu. Synkronointimerkki on 128 tai 56 bitin mittainen bittikuvio, jonka tarkoituksena on nimensä mukaisesti synkronoida lähettävä ja vastaanottava asema toisiinsa. Tämän lisäksi se auttaa valitsemaan parhaan signaalin antavan antennin ja säätää vastaanottokellon. Pitkän kehyksen synkronointimerkissä on pelkkiä ykkösiä ja lyhyen kehyksen vastaavassa pelkkiä nollia. Alkulippu erottaa alkumerkin ja varsinaisen kehyksen toisistaan ja se on pitkässä ja lyhyessä kehyksessä kahden tavun mittainen. Alkumerkin jälkeen tulee PPDU-kehyksen otsikko, joka lähetetään lyhyessä kehyksessä 2Mbit/s nopeudella ja pitkässä 1Mbit/s nopeudella. Molemmat kehykset sisältävät seuraavat otsikkokentät: [2][27]

- Signaali, josta käy ilmi lähetettävän datakentän siirtoon käytettävä bittinopeus. [2][27]
- Palvelukenttä, joka sisältää pituuskentän, käytettävän moduloinnin ja kellon lukituksen. [2][27]
- Pituuskentän, joka sisältää lähetykseen varattavan ajan mikrosekunneissa. [2][27]
- Otsikon/otsakkeen tarkastussumman, jolla varmennetaan otsikon virheettömyys. Tämä ei kuitenkaan havaitse muita kehyksessä mahdollisesti olevia virheitä. [2][27]

Kehyksen viimeinen osa on datakenttä, jossa MPDU-kehys sijaitsee. PPDU-kehys sekoitetaan ja hajotetaan, jolloin lähetys muistuttaa satunnaiskohinaa. Lähettimellä ja vastaanottimella on käytössään sama polynomi, jolloin sekoitus ei vaikuta kehykseen ja sen sisältämään dataan. Lopuksi kehys lähetetään signaalikentän mukaisella nopeudella. [2][27]



Kuva 8: 802.11b DSSS:n konvergenssikerroksen PPDU-kehys [2]

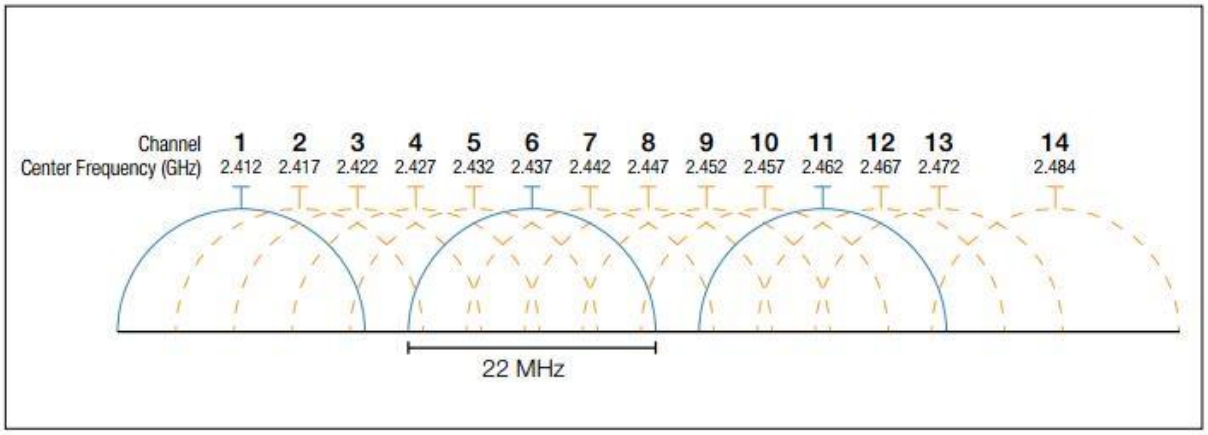
PMD-kerros määrittelee standardit, lähetystavat, bittinopeudet, kanavat, bittien hajotuksen alikanaville ja modulaatiotavat. 802.11-standardit käyttävät tiedonsiirtoon radiolähetystä ja hajaspektritekniikkaa. Hajaspektritekniikassa radiolähetys hajautetaan kantoaallon molemmille puolille laajemmalle alueelle, kuin bittinopeus vaatii. Tällä kompensoidaan vapaasti käytössä olevien taajuuksien häiriöiden vaikutusta. Tällöin pistemäinen häiriötaajuus ei vaikuta koko lähetysspektriin. 802.11-standardiin kuuluu taajuushyppely, jolla lähetystaajuutta hyppyytetään ennalta määritellyn kuvion mukaan.

Suorasekvenssitekniikassa DSSS:ssa bittijono hajautetaan laajalle taajuusalueelle ja lähetetään samanaikaisesti matemaattisten funktioiden perusteella. Lähetys sisältää tarpeetonta tietoa, joten vaikka 50% alikanavien tiedoista muuttuu, voidaan alkuperäinen bittikuvio toistaa. 802.11b käyttää bittinopeudesta riippuen joko Barker- tai CCK-hajautusta. Alemmat bittinopeudet käyttävät Baker-hajautusta, jossa lähtevät bitit lasketaan yhteen yhdentoista bitin Baker-koodin kanssa. Saadussa lähetteessä on 11 alkiota jokaisesta databitistä, jolloin taajuusalue on 22-kertainen verrattuna alkuperäiseen. Vastaanottaja laskee vastaanottamansa alkiojonon yhteen Baker-koodin kanssa, josta se saa alkuperäiset databitit. Baker-koodilla hajautettu alkiojono muistuttaa mahdollisimman paljon satunnaiskohinaa, jotta se aiheuttaisi mahdollisimman vähän häiriöitä muille järjestelmille. Baker-hajautusta ei nykyään juuri käytetä, sillä tiedonsiirtonopeudet ovat kasvaneet sille liian suuriksi. [2][27]

CCK komplementaarikoodiavainnuksessa käytetään ensin 11-bitin hajautusta, jonka jälkeen alkiobitit ryhmitetään kahdeksan alkion koodisanoiksi. Mahdollisia sarjoja on 256, mutta niistä käytetään vain muutamaa, jolla koodataan neljän tai kuuden bitin sanoja. Vastaanottajan on helppo erottaa koodisanat toisistaan myös häiriöllisissä olosuhteissa ja monitiehäipymisen

esiintyessä. Kanavan taajuusalue on 22Mbit/s. 5,5Mbit/s nopeudella alkiovirrasta erotetaan neljän bitin lohkoja, joista kaksi koodataan nelitasoisella vaihe-erolla ja loput sopivasti valituilla kahdeksan bitin koodisanoilla. 11Mbit/s nopeudella alkiovirrasta erotetaan kahdeksan bitin lohkoja, joista kaksi koodataan DQPSK-vaihe-erolla ja loput kuusi kahdeksan bitin koodisanoilla. Ylempien bittinopeuksien symbolikello on 1375 Msym/s, jolloin 2+6 bitin lohkoilla nopeus on 11Mbit/s ja 2+2 lohkoilla 5,5 Mbit/s. Hitaimmilla nopeuksilla käytetään DBPSK-modulaatiota, jolloin kantoaallon vaihetta käännetään 180 astetta ykkösbitin alkaessa. Nopeammilla bittinopeuksilla käytetään DQPSK-modulointia, jolloin kantoaallon taajuutta käännetään 0, 90, 180 tai 270 astetta. [2][27]

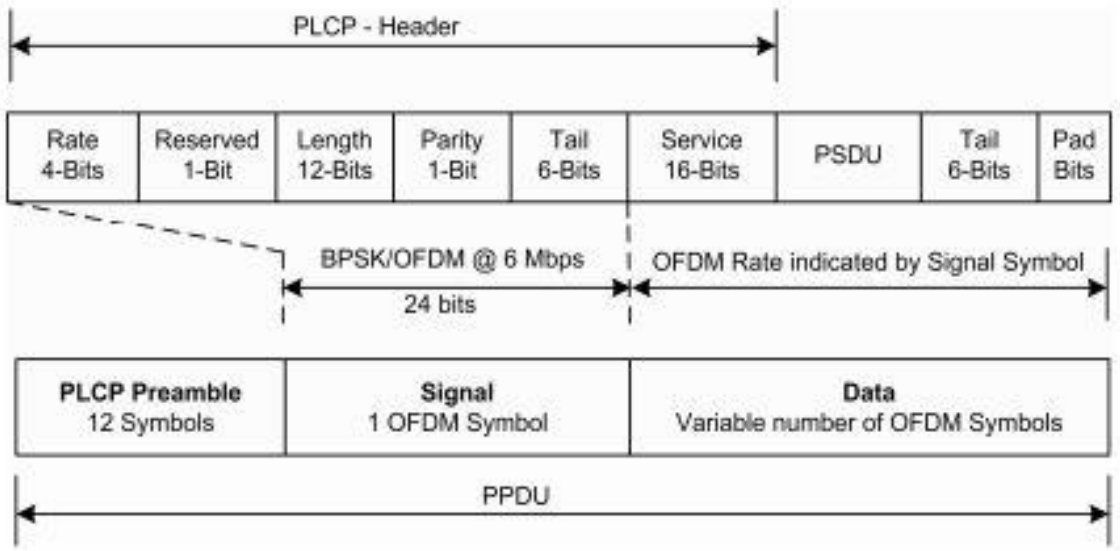
802.11b:n ja 802.11g:n käyttämä vapaa 2,4GHz:n taajuusalue on jaettu 14 kanavaan, jotka sijaitsevat 5Mhz välein. Kanavat ovat 22MHz leveitä, joten ne menevät päällekkäin häiriten toisiaan. Lähekkäin olevissa WLAN-verkoissa tulisi käyttää mahdollisuuksien mukaan kanavia, jotka eivät mene toistensa kanssa päällekkäin häiriöiden välttämiseksi. Euroopassa on käytössä vain kanavat 1-13. [27][39]



Kuva 9: 2,4GHz kanavat. [39]

Uudempien 802.11-standardien fyysinen kerros käyttää monikantoaaltomodulointia (OFDM). Myös OFDM-tekniikassa siirrettävä data jaetaan rinnakkaiskäytössä oleviin eri taajuuksilla toimiviin alikanaviin. OFDM:ssa alikanavien välissä ei ole varokaistaa, vaan kanavien taajuusspektrit on valittu siten, että jokaisen alikanavan keskitaajuudella muiden kanavien spektri on nolla. OFDM-modulaatiossa lähetettävä signaali muodostetaan osakanavista nopeaa Fourier-muunnosta käyttämällä. Tällöin ainoastaan lähetyssignaalin spektri merkitsee. Vastaanotin laskee alikanavien taajuusspektrien amplitudit ja muodostaa näiden tiedoista alkuperäisen bittijonon. OFDM:n PPDU-kehys koostuu alkumerkistä ja otsikosta. Loogisessa kehyksessä on tämän lisäksi loppumerkin bittejä, jotka liittyvät käytettyyn koodaukseen. Fyysisen kehyk-

sen otsikko on yhden symbolin signaalikenttä, jota on laajennettu loogisella tasolla siten, että se käyttää myös datakentän bittejä otsikolle. Alkumerkki koostuu 12 OFDM-symbolista, joiden avulla synkronoidaan lähettimen ja vastaanottimen ajastimet. Fyysisen PPDU-kehyksen otsikko on 1 symbolin signaalikenttä, joka kertoo nopeustiedon ja MAC-kehyksen pituuden, sekä hännän, jota tarvitaan konvoluutiokoodauksen avaamiseen. Looginen PPDU-kehys sisältää yllämainittujen lisäksi palvelukentän ja vaihtuvamittaisen loppumerkin, jotka sisältyvät fyysisen kehyksen datakenttään. Datakentän bitit sekoitetaan ennen lähetystä. Loppumerkki sisältää varsinaisen loppumerkin, jota tarvitaan konvoluutiokoodauksen lopettamiseen, sekä vaihtuvamittaisen täytteen, jolla täytetään datakenttä niin, että se vastaa OFDM-koodauksen tarvitsemaa lohkonpituutta. [2][21][27]



Kuva 10: MPDU:n konvergenssikerroksen PPDU-kehys [2]

PMD-kerroksella lähetetään 250000 symbolia sekunnissa käyttäen 48 alikanavaa. Käytetty modulaatiomenetelmä vaikuttaa symbolin sisältämien bittien määrään ja osa biteistä käytetään konvoluutiosuhteen mukaan virheenkorjaukseen. Tällöin bittinopeudeksi tulee 6-54Mbit/s. 6 ja 9Mbit/s nopeuksilla koodataan yksi bitti/merkki ja alikanavan biteistä käytetään puolet tai yksi neljäsosa virheenkorjaukseen. 12 ja 18Mbit/s nopeuksilla koodataan kaksi bittiä merkkiä kohden, 24 ja 36Mbit/s neljä bittiä merkkiä kohden ja suurimmalla nopeudella kuusi bittiä merkkiä kohden. Käytettävä modulaatio on joko BPSK, QPSK, 16-QAM tai 64-QAM.

Kun koodataan kuusi bittiä yhteen merkkiin ja merkkejä lähetetään rinnakkain 48 kanavalla, saadaan 6*48=288 bittiä/lähetys. Suurimmalla nopeudella 3/4 biteistä käytetään datalle ja

loput virheen korjaukseen. Tällöin jokaisella lähetyskerralla liikkuu 3/4*288=216 bittiä. Kun symbolinopeus on 250000 symbolia sekunnissa, tulee lopulliseksi maksiminopeudeksi 216bit*250000 1/s =54Mbit/s. [2][21][27]

802.11g verkot käyttävät konvoluutiokoodausta kapeakaistaisten häiriöiden vaikutusten poistamiseen. Virheenkorjauksen hyötysuhde kerrotaan databittien suhteena kokonaisbittimäärään. Esimerkiksi 3/4 tarkoittaa, että kolme neljäsosaa siirrettävistä biteistä on hyötydataa. Mitä pienempi suhde, sitä parempi virheensieto, mutta vastaavasti sitä pienempi hyötynopeus. [2][21][27]

802.11n-standardi käyttää samaa OFDM-modulaatiota, kuin 802.11g, mutta se toimii 2,4GHz:n kaistan lisäksi myös 5GHz:n kaistalla. 802.11n:n nopeutta lisää merkittävästi se, että sillä on käytössään 40MHz:n kanavat ja MIMO tekniikka. Lisäksi se käyttää kehysten yhdistämistä, jolloin lähetyksissä olevat otsikkotiedot vähenevät ja hyötydatan määrä kasvaa. MIMO mahdollistaa useamman antennin kautta tapahtuvan yhtäaikaisen lähettämisen ja vastaanottamisen. Yhtäaikaisten lähetteiden määrää rajoittaa lähetyspään ja vastaanottopään antennien määrä. Se kummassa on vähemmän antenneja luo rajoitteen. MxN=Z kertoo radion kyvystä signaalien vastaanottoon ja lähettämiseen. M tarkoittaa lähettävien antennien maksimimäärää, N tarkoittaa vastaanottavien antennien maksimimäärää ja Z kertoo yhtäaikaisten erillisten signaalien maksimimäärän laitteessa. 40MHz kanavien käyttö kaksinkertaistaa fyysisen datan lähetysmäärän verrattuna 20MHz leveisiin kanaviin. 40MHz kanavien käyttö ei saa kuitenkaan häiritä muita samoilla taajuuksilla toimivia laitteita. Suurimmilla nopeuksilla koodaussuhde on 5/6, kun se edellisessä standardissa oli maksimissaan 3/4. Modulointityyppeinä käytetään edelleen BPSK, QPSK, 16-QAM ja 64-QAM. 802.11ac-standardissa MIMO-kykyä on edelleen kehitetty ja käyttöön on otettu kaistanleveydet 160MHz asti. [22][23][39]

2.4. Langattomaan verkkoon kohdistuvat uhat.

Mikäli langaton lähiverkko on suojaamaton ja verkon SSID on tiedossa, voidaan verkkoon liittyä millä tahansa päätelaitteella. Suojaamattomaan verkkoon pystyy liittymään ilman minkäänlaista käyttäjän tunnistusta. Vaikka SSID olisi piilotettu, voidaan verkko silti havaita, koska se käyttää tiedonsiirtoon radiosignaaleja ja jo verkkoon liittyneet asemat lähettävät SSID:n selväkielisenä radioteitä pitkin. Kaikki radioliikenne yhteyspisteen ja pääteaseman välillä on salaamatonta, joten jos sovelluskerros ei erikseen salaa lähetystä, voi ulkopuolinen taho päästä siihen käsiksi. Verkkoon päässyt taho voi käyttää verkossa olevia laitteita ja yrittää murtautua jokaiseen verkossa olevaan työasemaan, mikäli niitä ei ole suojattu erikseen palomuurilla. Myös yhteyspisteen konsoliportti löytyy, mikäli verkkoon päästään sisään. Tämä on suojattu salasanalla, mutta mikäli sitä ei ole muutettu tehdasasetuksista, on se helppo arvata tai selvittää valmistajan sivuilta. Tämän jälkeen käyttäjä pääsee muokkaamaan yhteyspisteen asetuksia vapaasti ja jälkeä jättämättä. Yhteyspiste voidaan myös varastaa ja korvata uudella. Verkkoa käyttävät työasemat voidaan huijata ottamaan yhteys uuteen yhteyspisteeseen, jolloin niiden salasanat ja käyttäjätunnukset voidaan varastaa. Lisäksi langatonta verkkoa voidaan häiritä sen läheisyydestä esimerkiksi lähettämällä runsaasti liittymispyyntöjä. [27][28]

Langattomaan verkkoon kohdistuvat uhkat ovat joko passiivisia tai aktiivisia. Passiivisiin uhkiin kuuluu liikenteen salakuuntelu, jolla voidaan kerätä tietoa suoraan verkossa liikkuvasta datasta tai tietoa, joka auttaa murtautumaan itse verkkoon. Salakuuntelua on mahdoton havaita ja sen estäminen on hyvin vaikeaa. Verkon liikennettä voidaan salakuunnella ja analysoida jälkeenpäin ja kaivaa sieltä esiin turva-asetuksia ja salausavaimia. Aktiivisia uhkia ovat ne, joissa verkkoon lähetetään dataa tai signaaleja. Verkkoa voidaan häiritä radiolähettimellä, joka toimii samoilla taajuuksilla tai sitä voidaan ylikuormittaa palvelunestohyökkäyksillä. Langattomassa verkossa liikkuvaa dataa voidaan myös muokata niin, että osapuolet luulevat keskustelevansa toistensa kanssa, vaikka tosiasiassa kaikki liikenne kulkee kolmannen osapuolen kautta. Verkkoon voidaan myös yrittää murtautua sisään selvittämällä sen salausavain. Mikäli salausavain saadaan selville, voidaan kaikki yhteyspisteen kautta kulkeva liikenne lukea selkokielisenä. Useasti verkkoon kohdistuvan uhkan päämääränä on verkkoon tunkeutuminen ja sen sisällä oleviin laitteisiin tai tietoihin käsiksi pääseminen. [27]

Hyökkääjän verkkoon kohdistamat toimet alkavat yleensä skannaamalla olemassa olevia verkkoja. Hyökkääjä yrittää löytää verkoista sen, mihin on tarkoitus hyökätä. Verkkoja voi etsiä joko passiivisesti tai aktiivisesti. Aktiivisessa etsinnässä lähetetään verkkokyselyitä joko yleisesti, johon alueella olevat verkota vastaavat, tai kohdistetusti jollekin tietylle verkolle. Aktiivisella etsinnällä ei nähdä muuta kuin verkkopyyntöjä tai niin sanottuja majakoita, joilla yhteyspisteet ilmoittavat olemassaolostaan. Passiivisessa etsinnässä verkoille ei lähetetä pyyntöjä, vaan pelkästään kuuntelevat tiettyä kanavaa ja analysoivat siellä kulkevaa liikennettä. Samalla kanavalla voi toimia useita verkkoja yhtä aikaa, jolloin niiden kaikkien liikenne näkyy kuuntelijalle. Laitteet, joilla kuuntelua voidaan toteuttaa maksavat korkeintaan muutamia satasia, joten lähes kuka vaan voi sellaisia hankkia. [20]

Erilaisia hyökkäysmuotoja on monia. Verkon käyttäjien todennuksia voidaan purkaa, joka pakottaa käyttäjän liittymään uudestaan verkkoon. Pakottamalla käyttäjä liittymään uudestaan verkkoon, saadaan selville verkon nimen (SSID), koska se sisältyy selväkielisenä yhteysviestiin. Tämän lisäksi todennuksia purkamalla voidaan käyttäjältä estää yhteyspisteenkäyttö, jolloin kyseinen hyökkäystapa toimii palvelunestohyökkäyksenä. Todennuksen purkua käytetään myös siinä tilanteessa, kun halutaan, että käyttäjä suorittaa todennuksen uudestaan. Tätä halutaan silloin, kun hyökkääjä haluaa saada haltuunsa käyttäjän ja yhteyspisteenvälisen todennuksen. Useimmin neljän suunnan kädenpuristuksen. Sitä kautta voidaan päästä käsiksi haluttuihin tietoihin. Yleisesti todennuksen salakuuntelu, on monissa verkkohyökkäyksissä toiminnan ensimmäinen vaihe. [20]

Hyökkääjä voi myös tunkeutua verkkoon, jossa käytetään MAC-osoitteiden suodattamista. Tämä käy helposti käyttämällä passiivista kuuntelua, jonka avulla tiedustellaan jonkin jo verkossa olevan laitteen MAC-soite, joka sitten otetaan käyttöön. Nämä kaksi edellä mainittua tapaa eivät ole varsinaisia hyökkäyksiä verkon suojausta vastaan, vaan niillä voidaan liittyä suojaamattomiin verkkoihin, joita on yritetty piilottaa. [20]

Vanhanaikaista WEP-suojausta vastaan on olemassa useita hyökkäyksiä. Niiden tarkoituksena on hankkia WEP-avaimet, jonka jälkeen hyökkääjällä on vapaa pääsy verkkoon. Yksinkertaisimmillaan WEP-avaimen voi hankkia muokkaamalla tiettyjen valmistajien yhteyspisteiden SSID:tä. FMS-hyökkäyksessä käytetään hyväksi WEP-salauksen heikkoja avaimia. Siinä keskitytään RC4 salauksen ensimmäisen tavun selvittämiseen heikkojen avainten sattuessa kohdalle. Kun ensimmäinen tavu on saatu selville, pyritään sen avulla selvittämään seuraava ja niin edelleen. Todennäköisyys arvata seuraava tavu oikein on 5%. KoreK hyökkäyksessä keskitytään myös joko ensimmäisen tai kahden ensimmäisen tavun selvittämiseen tai rajaamaan etsittävien arvojen määrää. PTW hyökkäys kehitti alkuperäistä FMS hyökkäystä siten, että se toimi myös muita kuin heikkoja avaimia vastaan. Hyökkäyksellä onnistuttiin selvittämään salausavain 50% todennäköisyydellä 40000 kehyksestä ja 95% todennäköisyydellä 85000 kehyksestä. Tarvittava määrä kehyksiä voidaan saada alle minuutissa. [12][20][31]

Uudemman WPA-salauksen murtaminen ei ole enää niin helppoa kuin vanhemman WEP-salauksen, mutta sitäkin vastaan on mahdollista hyökätä. Lähtökohtana hyökkäyksille on niin sanotun neljän suunnan kädenpuristuksen tiedustelu. Hyökkääjä haluaa tietoonsa verkon SSID:n, molempien osapuolten MAC osoitteet, sekä kädenpuristuksessa yhteyspisteen lähettämän ANoncen ja käyttäjän lähettämän SNoncen. Hyökkääjä tarvitsee myös eheydenvarmistamiseen käytettävän MIC-avaimen. Kaikki nämä tiedot saa haltuunsa passiivisella kuuntelulla, joten hyökkääjä ei paljasta itseään. Kun käytetään passiivista menetelmää, joudutaan odottamaan, että verkkoon liittyy joku. Mikäli tähän ei ole aikaa, voidaan jokin jo verkossa oleva käyttäjä potkaista verkosta ulos ja odottaa, että hän liittyy siihen uudestaan, jolloin 4-way handshake tehdään uudelleen. Kun kädenpuristus on tiedusteltu, täytyy avaus murtaa brute force menetelmällä, joka voi kestää salasanan vahvuudesta riippuen pitkään. Menetelmä vaatii tietokoneelta runsaasti laskentatehoa. Yleisesti ottaen WPA:n ennalta jaettu avain on helpompi murtaa, kuin WPA Enterprise, koska salasana pystyy samana pitkiä aikoja, eikä se ole välttämättä niin monimutkainen. [20]

Vaikka hyökkääjä saisikin haltuunsa kädenpuristuksessa määritettävän master -salausavaimen, tai tietäisi verkon salasanan, ei hän silti pysty lukemaan muiden verkonkäyttäjien liikennettä niiden avulla. Jokainen käyttäjä luo yhteyspisteen kanssa jokaista sessiota varten master-avaimen lisäksi sessiokohtaiset avaimet, jotka ovat jokaisella käyttäjällä erilaiset. Mikäli hyökkääjä haluaa päästä käsiksi kaikkeen verkon liikenteeseen, tulisi hänen murtaa jokaisen käyttäjän ja yhteyspisteen välinen kädenpuristus saadakseen kaikki tarvittavat avaimet. Tämä tietysti onnistuu, mutta vie aikaa. [20]

WPA Enterprise voi käyttää todennukseen useita eri todennustapoja. Todennus tapahtuu ennen varsinaista neljän suunnan kädenpuristusta. Mikäli WPA Enterprisea kohtaan halutaan hyökätä, täytyy ensin murtaa todennuksessa tapahtuva EAP -kädenpuristus. EAP -kädenpuristuksesta selviää, mitä EAP -tyyppiä todennuksessa käytetään, joka auttaa varsinaisessa hyökkäyksessä. EAP -kädenpuristuksesta voi selvitä käyttäjänimi, jolla yhteyttä muodostetaan. Käyttäjä voi tukea useampaa todennustyyppiä, joten on tärkeää, että koko kädenpuristus saadaan kuunneltua, jotta saadaan selville mikä loppujen lopuksi on käytössä. Riippuen käytettävästä EAP -todennuksesta, se voidaan joko murtaa helposti tai ei lainkaan. Helposti murrettava todennus on LEAP, kun taas EAP-TLS on mahdoton murtaa. [20]

Nykyisin käytettävät suojausmenetelmät ovat niin hyviä, että verkkoihin murtautuminen kestää pitkiä aikoja ja vaatii tehokkaita työkaluja. Tästä syystä Hyökkäykset ovat siirtyneet OSI-mallin ylempiin kerroksiin ja hyväksikäyttävät erilaisia sovelluskerroksen sovelluksia, joiden kautta muokataan liikenteen kulkua haluttuun suuntaan. Tällaisia tapauksia ovat muun muassa Flash ja Java -sovelluksista löytyvät tietoturva-aukot, joiden avulla kohteena olevaan laitteeseen saadaan ujutettua haluttuja toimintoja. [20]

3. LANGATTOMAN LÄHIVERKON SUOJAAMISEEN KÄYTETTÄVÄT MENETELMÄT

3.1. Käyttäjän todennus

Langattomiin verkkoihin liityttäessä tehdään käyttäjän tunnistus. Tunnistus tehdään ennen kuin käyttäjä voi kommunikoida verkon kanssa. Tunnistuskeinoja ovat: Avoin tunnistus MAC-osoitetunnistus, WEP-tunnistus, EAP- ja kevyempi LEAP-tunnistus, sekä WPA:n käyttämä niin sanottu fourway handshake. [9][27][40]

3.1.1 MAC-osoitetunnistus

MAC-osoitetunnistuksen ideana on se, että yhteyspisteelle on manuaalisesti määritelty MAC-osoitteet, joilla on lupa liittyä verkkoon. Mikäli verkko on iso ja siihen liittyviä päätelaitteita on paljon, on osoitelistan ylläpito ja käyttö hankalaa. Tämän lisäksi MAC-osoitteet liikkuvat verkossa salaamattomina. Verkkoa käyttävän päätelaitteen MAC-osoite voidaan tiedustella ja tämän jälkeen sitä voidaan käyttää verkkoon sisälle pääsyy. MAC-osoitetunnistus ei siis varsinaisesti ole suojauskeino vaan ennemminkin keino rajoittaa verkossa olevien laitteiden määrää. [9][27][40]

3.1.2 WEP-todennus

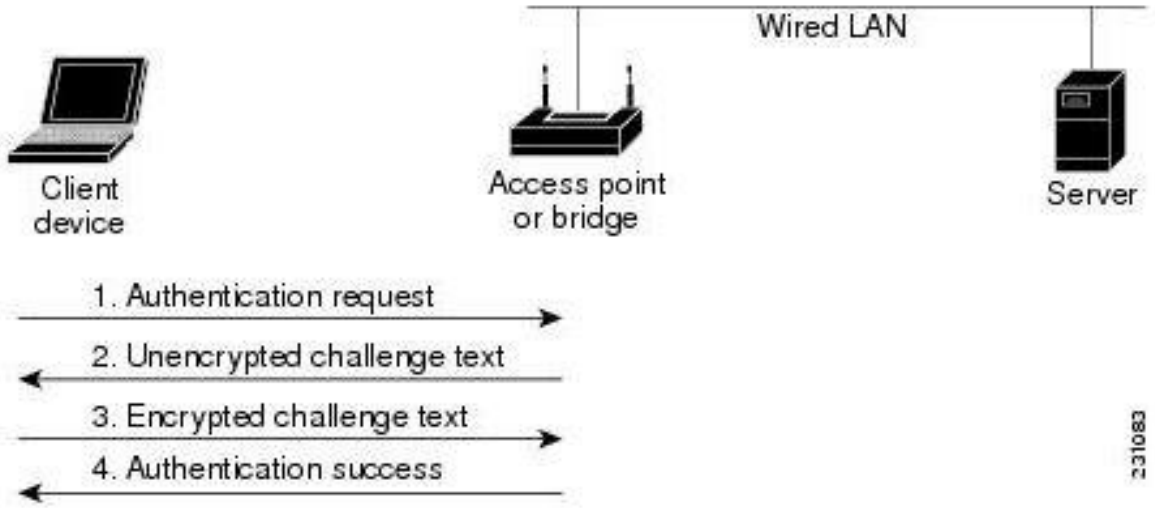
WEP on siirtokerroksen salausmenetelmä ja sen käyttö on vapaaehtoista. Salaus on symmetrinen ja kaikille asemille on määriteltävä sama avain kuin yhteyspisteelle. Salausavaimia on kahden kokoisia: 40- ja 104-bittinen. Niihin lisätään vielä 24 bitin alustusvektori. WEP perustuu jaetun avaimen menetelmään, jolloin todennus tapahtuu seuraavan kaavan mukaan: [9][27][40]

- Päätelaite lähettää tunnistuspyynnön, jossa se kertoo tukevansa jaetun avaimen tunnistusta. Hallintakehyksen sekvenssinumero on 1. [9][27][40]

- Yhteyspiste lähettää päätelaitteelle satunnaisen haastetekstin 802.11-hallintakehyksessä. Sen tunnistusalgoritmiksi ilmoitetaan jaetun avaimen tunnistus, tilakoodiksi onnistunut, haastetekstiksi satunnainen merkkijono ja sen sekvenssinumero on 2. [9][27][40]

- Päätelaite lähettää vastauksena takaisin saman tunnistusalgoritmin ja haastetekstin, jotka on salattu päätelaitteen WEP-avaimella. Tässä kohtaa sekvenssinumero on 3. [9][27][40]

- Yhteyspiste purkaa vastaanottamansa informaation ja vertaa sitä alkuperäiseen lähetteeseen. Jos tulos on sama, ovat myös salausavaimet samat ja todennus hyväksytään lähettämällä kuittaussanoma. Mikäli tulos on eri, lähetetään epäonnistunut syykoodi. Sekvenssinumero on 4. [9][27][40]



Kuva 11: WEP-todennuksen vaiheet [9]

WEP-tunnistuksen haaste on se, että kaikilla päätelaitteilla pitää olla käytössä sama avain kuin yhteyspisteellä. Yhteyspisteeseen ja työasemiin voidaan määritellä samanaikaisesti neljä WEP-avainta. WEP-salaus on nykyään helppo murtaa, sillä sen tietoturvassa on aukkoja. Mikäli WEPiä käytetään vain tunnistukseen, se ei anna murtautujalle paljoa lähtödataa. [9][27][40]

3.1.3 EAP-tunnistus

EAP-järjestelmään kuuluu päätelaitteen ohjelmisto, verkon reunalla oleva yhteyspiste ja tunnistuspalvelin. Päätelaite ja yhteyspiste keskustelevat keskenään EAPOW-protokollalla. Yhteyspiste ja todennuspalvelin keskustelevat halutulla tunnistusprotokollalla. EAP-tunnistus noudattaa seuraavaa ketjua: [9][27]

- Päätelaite liittyy yhteyspisteeseen MAC-osoitteellaan, jolloin sille välitetään vain EAP-liikennettä. Tässä vaiheessa suoritetaan 802.11:n avoin tunnistus. [9][27]

- Aluksi anoja, tässä tapauksessa päätelaite, lähettää EAPOL-start sanoman yhteyspisteelle, jonka jälkeen yhteyspiste kysyy käyttäjätietoja. [9][27]

- Käyttäjä kirjoittaa päätelaitteella käyttäjätunnuksen ja salasanan. Salasanasta lähetetään eteenpäin vain tiiviste. Tämän jälkeen yhteyspiste tarkastaa pitääkö käyttäjä tun-

nistaa. Käyttäjätiedot lähetetään EAP-sanomana eteenpäin ja lopulta RADIUS-attribuuttina tunnistuspalvelimelle. [9][27]

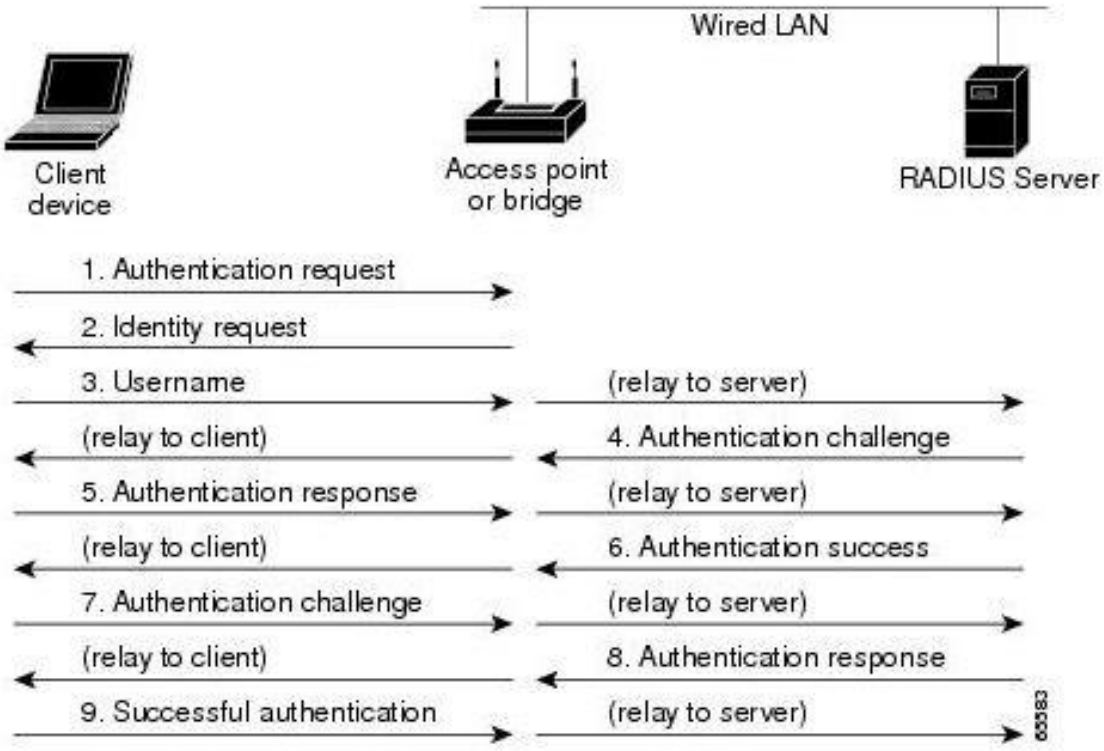
- Tunnistuspalvelin lähettää päätelaitteelle haastepaketin, joka sisältää satunnaisen merkkijonon ja salaisella avaimella salatun haasteen. Haaste välitetään päätelaitteelle EAP-pyynnössä. [9][27]

- Päätelaite lukee käyttäjän salasanan ja salakirjoittaa sillä haastejonon. Tämä lähetetään EAP-vasteessa RADIUS-pyyntönä eteenpäin. [9][27]

- RADIUS-palvelin salaa lähettämänsä haasteen käyttäjän salasanalla ja vertaa sitä vastaanottamaansa sanomaan. Mikäli ne täsmäävät, oli avain oikea ja käyttäjä voidaan liittää verkkoon. Päätelaitteelle lähetetään EAP-success-sanoma. Samalla päätelaitteelle lähetetään myös istunnon WEP-avain, jota voidaan vaihtaa määräajoin tietoturvan parantamiseksi. [9][27]

- Yhteyspiste lähettää käyttäjälle myös toisen WEP-avaimen, jota käytetään ryhmä-, ja yleislähetyskehyksille. Avain on salattu istuntoavaimella. [9][27]

- Kun käyttäjä purkaa yhteyden, päätelaite lähettää uloskirjaussanoman, jolloin yhteyspiste lopettaa päätelaitteen kanssakäymisen. [9][27]

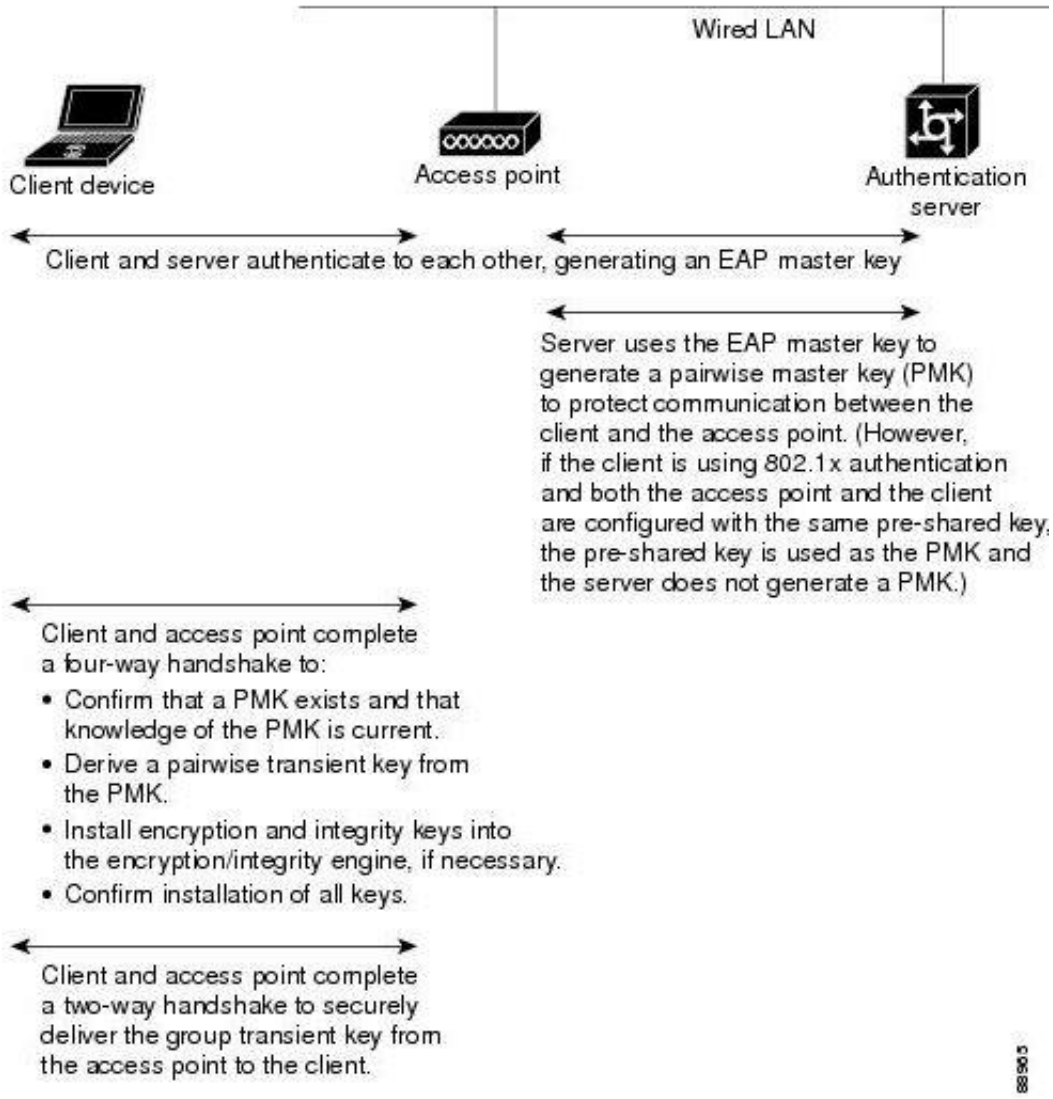


Kuva 12: EAP-tunnistuksen vaiheet. [9]

Riippuen käytettävästä EAP-tunnistusmenetelmästä voidaan suorittaa myös kaksisuuntainen tunnistus, jolloin päätelaite voi tunnistaa myös yhteyspisteen. Tällöin voidaan välttyä salasanojen urkkimiselta väärennetyllä yhteyspisteellä. Mikäli suoritetaan kaksisuuntainen tunnistus, päätelaite suorittaa yhteyspisteelle samanlaisen tunnistuksen, kuin yhteyspiste on päätelaitteelle tehnyt. [9][27]

3.1.4 WPA-tunnistus, niin sanottu four-way handshake

WPA toimii joko ennalta jaetun avaimen avulla, tai ilman. WPA-avainten hallintaa käyttäen tehty tunnistus toimii EAP-tunnistuksen mukaan. WPA-tunnistuksessa yhteyspiste ja päätelaite luovat yhteisen master-avaimen, jonka avulla tunnistus tapahtuu. Tätä avainta osapuolet eivät kuitenkaan paljasta toisilleen, vaan ne salaavat ja purkavat sen avulla viestejä, joilla ne todistavat toisilleen tietävänsä avaimen. Master-avain on istuntokohtainen. [3]

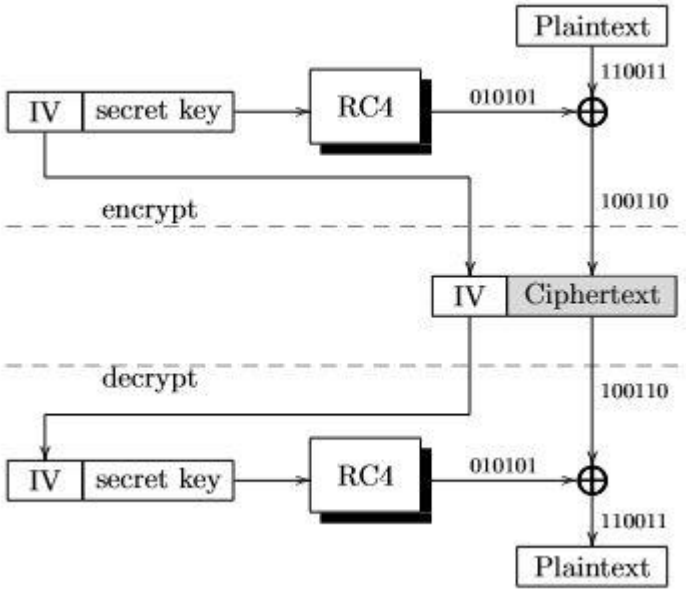


Kuva 13: WPA-tunnistuksen vaiheet [9]

3.2. WEP-salaus

3.2.1 Alkuperäinen WEP-salaus

802.11-standardin alkuperäinen salausmenetelmä oli 40 bitin jaettua avainta käyttävä WEP. Avaimen pituutta laajennettiin 104 bittiin, mutta se on silti riittämätön nykyaikaisille työasemille. Salauksen muodostaminen tapahtuu samalla tavalla molemmilla 40 ja 104-bitin avaimilla. WEP käyttää RC4-jonosalausta, jossa salausavain on yhtä pitkä kuin salattava tavujono. WEP-avain laajennetaan 24 bitin selväkielisellä alustusvektorilla ja RC4 avaimella generoidaan tavujonon mittainen RC4-avainvuo. Alustusvektori on selväkielinen siitä syystä, että vastaanottaja voisi käyttää samaa RC4-avainta. Selväkielisestä tavujonosta lasketaan nelitavuinen ICV-tiiviste, jolla taataan kehyksen eheys. Se lisätään WEP-kehykseen ja salattavan datan perään. Avainjono ja salattava data lasketaan yhteen bitti bitiltä ja saatu salattu tavujono viedään WEP-kehykseen. Kehys sisältää myös avaintunnuksen, joka kertoo mitä neljästä WEP-avaimesta käytetään. [6][10][27]



Kuva 14: WEP-salauksen toiminta. [10]

WEP-salauksessa on runsaasti tietoturvaongelmia:

- Samat WEP-avaimet määritellään kaikkiin samaa verkkoa käyttäviin laitteisiin. Avaimet näkyvät laiteasetuksissa selväkielisinä. Hyökkääjälle riittää siis pääsy jonkin verkossa olevan laitteen asetuksiin ja tämän jälkeen hän saa käyttöönsä verkossa käytettävät avaimet. Mikäli verkkoon halutaan uudet avaimet, on ne levitettävä kaikille laitteille samanaikaisesti, joka voi muodostua ongelmaksi isossa verkossa. [6][10][27]

- WEP-salatun verkon käyttäjäntunnistus on myös heikkoa. Käytössä on joko jaetun avaimen tunnistus tai avoin tunnistus, joka ei edes ole varsinainen tunnistus. Jaetun avaimen tunnistuksessa hyökkääjä voi kuunnella haastepaketin, joka on selväkielinen ja tämän jälkeen käyttäjän lähettämän salatun vastauksen, joiden perusteella hän voi päätellä avainvuon. Tämän avulla verkkoon voidaan lähettää salattuja paketteja ilman, että varsinaista avainta tiedetään. [6][10][27]

- IV-alustusvektori on salaamaton, joka voi auttaa mahdollista hyökkääjää. Alustusvektorin osoiteavaruus on vain 24 bittiä, jolloin sama vektori toistuu joka 17. miljoonas kerta. Eri alustusvektorien käyttöä peräkkäisille kehyksille ei ole vaadittu, eikä IV-vektoria käytetä estämään sanomien uudelleenlähetystä. IV-vektori myös paljastaa, milloin niin kutsuttua heikkoa avainta käytetään. [6][10][27]

- 40:n ja 104:n bitin salaus pystytään murtamaan nykyaikaisella laitteistolla yksinkertaisesti kokeilemalla eri avainkombinaatioita. Tätä kutsutaan brute force menetelmäksi. Lisäksi salauksen murtaminen helpottuu entisestään, jos murtaja saa vihjeitä sanoman ja avaimen sisällöstä. [6][10][27]

- Jaetun WEP-avaimen salausmenetelmät ovat myös hyvin alttiita analysoinnille, jos sama salausavain on käytössä useammin kuin kerran. Samaa IV-vektoria käyttävien pakettien salausavaimet ovat myös hyvin suurella todennäköisyydellä samat. [6][10][27]

- Mikäli hyökkääjä saa yhteyspisteen uudelleensalaamaan kaappaamansa WEP-kehyksen, tuloksena on alkuperäinen salaamaton paketti. Tämä johtuu salausfunktion symmetrisyydestä. [6][10][27]

- Tietyt alustusvektorit ovat heikkoja, joita voidaan käyttää apuna tietomurroissa. Niitä on 40-bitin avaimessa 0,008% ja 104-bitin avaimissa 0,02%. [6][10][27]

3.2.2 TKIP-parannukset

TKIP-parannukset ovat joukko algoritmeja, joilla WEP-salausta on parannettu. TKIP on lähinnä siirtymävaihe WPA2 suojaukseen, jolla varmistettiin, että laitteistot ovat yhteensopivia. TKIP sisältää seuraavan laisia parannuksia: [6][10][27]

- Kehyskohtaisesti generoitava 128-bitin salausavain, joka poistaa avainten uudelleenkäyttöongelman. [6][10][27]

- Alustusvektoria laajennettiin 48 bittiin ja sille määriteltiin vektorinvaihdot. Tällä tavalla heikkojen aloitusvektorien ongelma on saatu poistettua. [6][10][27]

- Ryhmälähetys- ja levitysviestikehysten salausavainta kierrätetään. Tällöin yhteyspiste vaihtaa näihin käytettyä avainta määräajoin. Oletusaika on 90 sekuntia, jolloin ei ehdi kertyä vaarallisen paljon ryhmälähetys- ja levitysviestejä. Levitysviestiavainten kierrätys vaatii työasemilta LEAP tai EAP-TLS-tunnistuksen. [6][10][27]

- Vahva sanoman eheyden tarkistus, jolla paljastetaan sanomien väärennysyritykset. Tällaisia ovat bittien järjestyksen muuttaminen ja lähde- tai kohdeosoitteen muuttaminen. [6][10][27]

TKIP-suojauksessa salaus aloitetaan yhteisellä 128-bitin aloitusavaimella, jota käyttävät molemmat osapuolet. Aloitusavain yhdistetään työaseman MAC- osoitteeseen ja kehyksen järjestysnumeron neljään merkitsevimpään bittiin. Tämä väliaikainen avain yhdistetään järjestysnumeroltaan kahteen alimpaan bittiin, jolloin saadaan kehyskohtainen avain. Näin ollen jokainen asema käyttää eri salausavainta, joka vaihtuu jokaiselle kehykselle. Kehyksen IV-kenttä salataan myös heikkojen alustusvektorien salaamiseksi. [6][12][27]

3.2.3 Eheyden varmistaminen

Langattomien verkkojen tietoturvassa on tärkeää kehysten eheyden varmistaminen. Tämä siksi, että radioteitse liikkuvaan tietoon pääsee helposti käsiksi ja sitä voidaan yrittää muuttaa matkan varrella. WEP-salauksessa eheys pyritään tarkastamaan ICV-sormenjäljen avulla. Se sisältyy WEP-kehykseen ja se on salattu. Ongelma on, että se muodostetaan samalla menetelmällä, kuin siirtokerroksen tarkastussumma. Tämä johtaa siihen, että sormenjäljen generointi muunnetulle sanomalle, on helppoa. Tässä tapauksessa käytetty CRC-tarkastusmenetelmä huomaa yksittäiset bittivirheet, mutta ei kykene havaitsemaan bittien järjestyksen muuttamista. Vaikka ICV-sormenjälki on salattu, ei se anna paljoa turvaa, kun itse WEP-salausmenetelmä on huono. WEP-salaukseen tehdyssä TIKP-parannuksessa myös eheyden tarkistusta parannettiin. TKIP käyttää MIC-eheydentarkistusta. Se laskee satunnaisesta siemenluvusta, MAC-otsikosta, sekvenssinumerosta ja hyötykuormasta 64-bitin sormenjäljen. Sormenjäljen täytyy täsmätä ja sanomien saapua oikeassa järjestyksessä tai kehys hylätään. WPA2:ssa eheydentarkistus tehdään TKIP:n MIC tarkistuksen tyylisesti, mutta käytössä olevan kehyksen muoto on erilainen. Kehystä kutsutaan CCMP-kehykseksi. [6][27]

3.3. WPA - TKIP

3.3.1 TKIP –kehysten lähetys ja vastaanotto

Kuten edellä mainittu TKIP-salaus kehitettiin parantamaan WEP-salausta. TKIP-salausta käyttää nykyisin vielä useat langattomat verkot ja tämän vuoksi myös WPA2-salaus tukee sitä. TKIP-salausta käyttävään verkkoon liitytään ja tehdään samanlainen käyttäjän tunnistus kuin WEP-salausta käyttävään verkkoon. Tapoja on kaksi, joko jaetun avaimen tunnistus tai avoin tunnistus. Nykyisin käytetään näistä jälkimmäistä. Se ei kuitenkaan tarjoa varsinaisesti turvallista tunnistusta, vaan lähinnä liittää laitteen yhteyspisteeseen. Todellinen tunnistus tapahtuu vasta myöhemmin. Kun yhteyspisteeseen on liitytty, lähettää käyttäjän työasema yhdistyspyynnön yhteyspisteelle. Tässä pyynnössä tapahtuu turvallinen tunnistus ja siinä työasema kertoo käytettävän salausprotokollan. Mikäli yhteyspiste tukee haluttua salausta, on yhdistys suoritettu. Kun käyttäjän työasema on tunnistettu, tapahtuu 4-way handshake, jossa neuvotellaan käytettävät salausavaimet istunnon ajaksi käyttäen IEEE 802.1X:ssa määriteltyjä EAPOL-avainkehyksiä. Tämän seurauksena syntyy 512-bittinen kahdenvälinen transient-avain, joka jaetaan käyttäjän ja yhteyspisteen välillä. Tästä avaimesta johdetaan 128-bittinen väliaikainen salausavain ja kaksi 64-bittistä viestien eheydenvarmistusavainta (MIC). MIC-avaimet jaetaan siten, että toinen on käytössä käyttäjältä yhteyspisteelle menevään liikenteeseen ja toinen vastakkaiseen suuntaan. MIC-avaimet uusitaan käyttäjän määrittämällä syklillä. Perus arvona avainten uusimiseen on yksi tunti. Kun kaikki avaimet on neuvoteltu, voidaan salattuja datakehyksiä lähettää käyttäjän ja yhteyspisteen välillä. Käyttäjä tai yhteyspiste voi keskeyttää yhteyden millä tahansa hetkellä lähettämällä yhteydenpurku- tai tunnistuksenpurkuviestin. Vanhemmissa versioissa nämä viestit olivat salaamattomia, jolloin mahdollinen hyökkääjä pystyi luomaan niitä, ja näin ollen katkaisemaan yhteyksiä käyttäjien ja yhteyspisteiden välillä. Myöhemmissä päivityksissä tämänkaltaiset hyökkäykset estettiin salaamalla johtokehykset. [6][12][32]

Lähetettäessä TKIP-kehystä, lasketaan ensin MIC -arvo MSDU-kehykselle. Tällä tavoin pyritään suojaamaan lähetettävän kehyksen eheyttä ja autenttisuutta. MIC -arvo lasketaan MSDU-kehyksestä niin sanotulla Michael algoritmilla. Laskettu MIC –arvo on kahdeksan tavun mittainen. Michael algoritmi itsessään ei kuitenkaan ole riittävän turvallinen, joten siihen on lisätty vastatoimia, joilla sen turvallisuutta on pyritty parantamaan. Lähetettävät MSDU –kehykset hajotetaan tarvittaessa pienemmiksi MPDU-kehyksiksi, joita hyväksytään yhteensä 16 kappaletta. Jokainen MPDU-kehys käy läpi WEP-paketoinnin, jotta TKIP toimisi myös vanhempien WEP –laitteiden kanssa. WEP-salauksessa kehykseen lisätään 32-bittinen ICV-arvo. Tämän jälkeen paketti salataan käyttäen RC4-salainta. Salausavain lasketaan yhtälöllä,

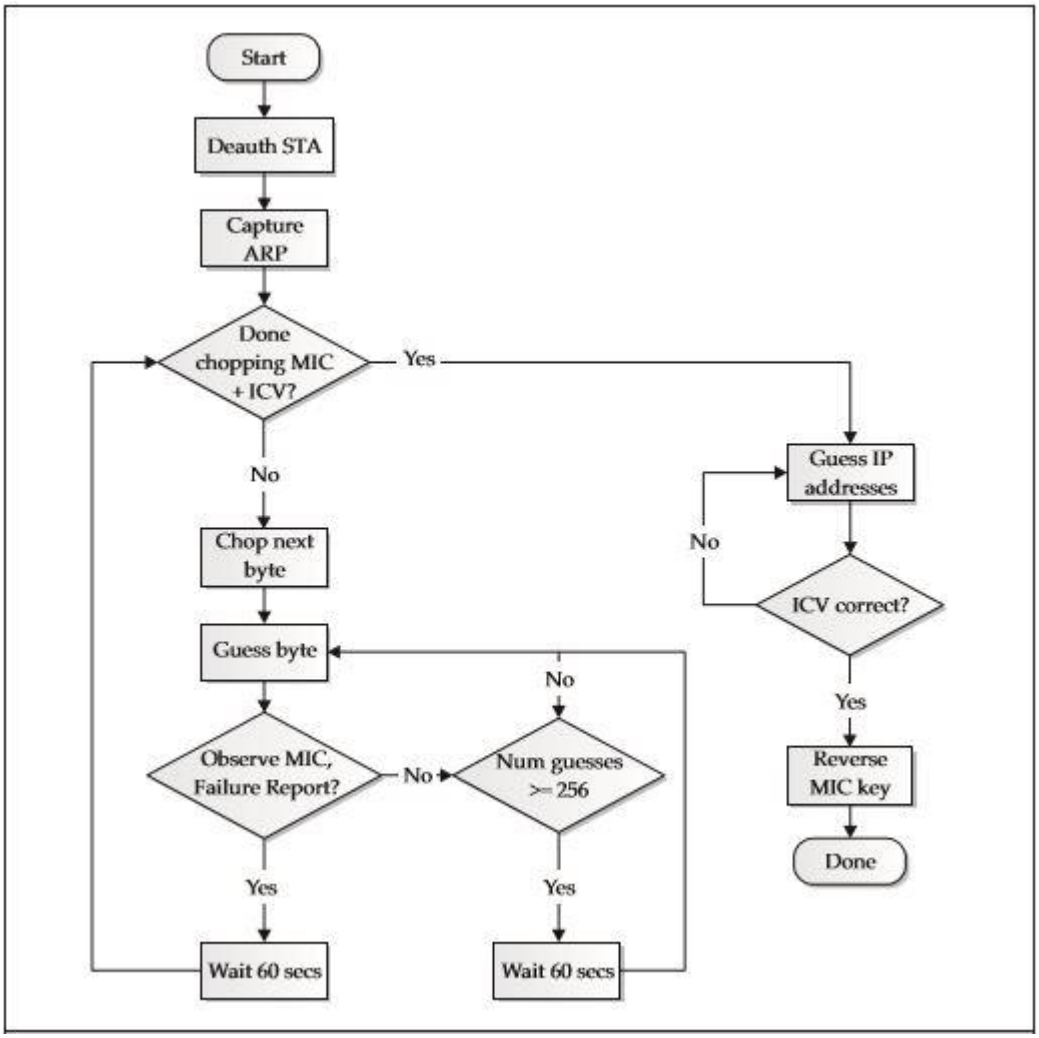
jossa käytetään väliaikaista avainta, lähettäjän MAC-osoitetta ja TKIP sekvenssinumeroa. Lopuksi tähän lisätään tavalliset 802.11 mukaiset otsikot joihin kuuluu TKIP sekvenssilaskuri, jonka luku nousee ylöspäin jokaisesta onnistuneesta MPDU –kehyksen lähetyksestä. Hyökkäysten ehkäisemiseksi vastaanotin pudottaa pois kehykset, joita ei vastaanoteta järjestyksessä. Jokainen lähetettävä paketti salataan käyttämällä eri salausavainta, joka on johdettu pääavaimesta. [6][12][32]

Vastaanotettaessa TKIP-kehystä käyttäjä tai yhteyspiste tarkistaa ensin, että TKIP sekvenssilaskuri on järjestyksessä. Mikäli näin ei ole pudotetaan kehys pois. Tämän jälkeen tarkastetaan ICV:n oikeellisuus. Jälleen kerran, jos se ei ole oikea, pudotetaan kehys pois. Kun kaikki MPDU:t on vastaanotettu ja koottu MSDU:ksi tarkastetaan MIC -arvo. Arvon ollessa oikein hyväksytään kehys ja TSC-laskuriin lisätään yksi. Mikäli MIC -arvo on väärä, alkavat vastatoimet. Mahdollinen hyökkäys MIC-avaimen selvittämiseksi, on lähettää vastaanottajalle useita vääriä paketteja, joilla on eri MIC-arvo ja toivoa, että jokin niistä on oikea. Mikäli oikean MIC-arvon sisältävä paketti löydetään, voidaan siitä johtaa kyseisen suunnan MIC-avain. Mikäli käyttäjä havaitsee vastaanotetussa MSDU:ssa väärän MIC arvon, lähettää se yhteyspisteelle virheraportin. Mikäli vastaanottajana on yhteyspiste, se ei lähetä virheraporttia käyttäjän suuntaan, vaan kirjaa virheen lokiin. Jos yhteyspiste havaitsee kaksi MIC –virhettä minuutin sisällä, kaikki TKIP:tä käyttävät yhteydet katkaistaan, eikä yhteyspiste enää lähetä tai vastaanota TKIP-salattua dataa seuraavaan minuuttiin. Minuutin jälkeen käyttäjät voivat jälleen yhdistää yhteyspisteeseen, jolloin kaikki avaimet luodaan uudestaan. [6][12][32]

3.3.2 TKIP:n kohdistuvat uhkat

TKIP-salausta kohtaan on olemassa erilaisia hyökkäyksiä. Yhtä ensimmäisistä kutsutaan Beck ja Tews hyökkäykseksi ja siihen pohjautuvia hyökkäyksiä on useampia. Beck ja Tews toimii purkamalla salauksen data-paketin tavu kerrallaan. Hyökkäys toimii siten, että ensin kaapataan yksi paketti, josta poistetaan viimeinen tavu. Tässä lyhennetyssä paketissa ICV-arvo on todennäköisesti väärä. Se voidaan kuitenkin korjata oikeaksi, mikäli tiedetään poistetun tavun salaamaton arvo. Tämä arvo saadaan kokeilemalla. Hyökkääjän täytyy kokeilla kaikki 2^8 mahdollista arvoa poistetulle tavulle. Oletettavasti vastaanottajalla on alempi TKIP sekvenssilaskurin numero, jolloin lähetetty paketti menee läpi. Tämän jälkeen vastaanottaja tarkistaa ICV arvon. Mikäli se on väärä, pudotetaan paketti pois. Mikäli arvo on arvattu oikein, se menee läpi ja vastaanottaja tarkistaa paketin MIC-arvon. Suurella todennäköisyydellä MIC-arvo on väärin, jolloin käyttäjä lähettää yhteyspisteelle virheilmoituksen. Oikea arvaus voidaan selvittää virheilmoituksia kuuntelemalla. Yhteyspiste ei ole haavoittuvainen tämänkaltaista hyökkäystä vastaan, koska se ei lähetä virheilmoituksia. Jotta vastatoimia ei laukaista, voi-

daan purkaa yksi tavu minuutissa. Koska koko paketin purkaminen näin vie liian kauan, keskittyy Beck ja Tews hyökkäys vain APR vastausten ICV ja MIC arvoihin. Näillä keinoin purkuun menee noin 12-15 minuuttia. Paketin loppusisältö arvataan. Kun arvausta verrataan purettuun ICV:n ja ne täsmäävät, voidaan olettaa, että arvaus on oikein. Kun ARP vastaus on saatu purettua, voidaan Michael algoritmia käyttää käänteisesti yhteyspisteeltä käyttäjälle suunnatun MIC avaimen laskemiseen. Tällä tavoin voidaan väärentää kolmesta seitsemään pakettia, joiden pituus on yhteensä sama tai pienempi kuin ARP –vastauksen. Näiden pakettien koko on maksimissaan 28 tavua. Kun MIC-avain on tiedossa ja lähetetystä kehyksestä voidaan päätellä, onko se ARP, EAPOL vai IP –kehys, saadaan lähetetyn datan määräksi 102 tavua. Lähetetyn kehyksen tyyppi voidaan päätellä muun muassa otsaketietojen perusteella. [12][20][32][31]



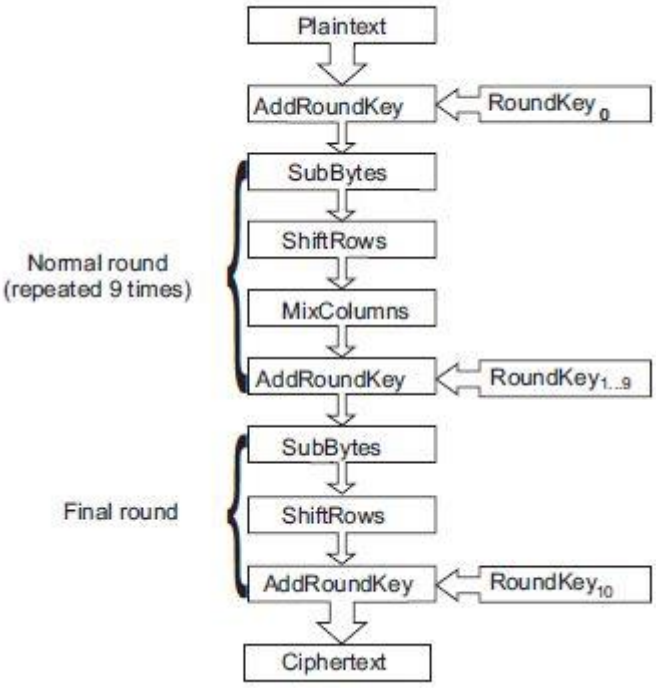
Kuva 15: Beck and Tews -hyökkäys [20]

Toinen mahdollinen hyökkäys on palvelunestohyökkäys, jossa kaapataan lähetetty paketti, muutetaan sen prioriteettinumeroa ja lähetetään se edelleen. Tällöin MIC-arvo ei täsmää. Kun tällaisia paketteja lähetetään kaksi minuutin sisällä, pudottaa yhteyspiste kaiken TKIP-liikenteen pois käytöstä minuutin ajaksi. Kun sama toistetaan minuutin välein, estyy kaikki kyseisen yhteyspisteen kautta kulkeva TKIP -salattu liikenne. Erilaisilla työkaluilla voidaan seurata TKIP liikennettä ja nähdä sieltä mm. MIC virheiden määrät ja muu salaamaton data, jota voidaan käyttää apuna hyökkäyksessä. [32]

Kolmas mahdollisuus on Brute Force -hyökkäys, jossa on tarkoituksena murtaa salausavain yksinkertaisesti arvaamalla se. Hyökkääjän tarvitsee tässä tapauksessa kaapata niin sanottu neljän suunnan kädenpuristus, jolla käyttäjä ja yhteyspiste tunnistuksen yhteydessä toteavat, että tietävät yhteisen master-avaimen, josta loput avaimet johdetaan. Kun kädenpuristus on kaapattu, voidaan loppuosa hyökkäyksestä tehdä offline-tilassa. Tämän jälkeen hyökkääjä alkaa arvailla salasanaa sattumanvaraisesti, jolloin salasanoja luodaan siten, että mahdollisia käytettävissä olevia merkkejä aletaan arvata järjestyksessä. Hyökkääjä voi myös käyttää arvauksiinsa ennalta määritettyä kirjastoa. Ottaen huomioon mahdollisten vaihtoehtojen määrän, tulisi kirjastojen olla todella suuria, jotta mahdollisuus löytää salasana niistä olisi olemassa. Mikäli murrettava salasana ei sisälly kirjastoon, ei sitä ole mahdollista arvata. Kahdenvälinen master-avain lasketaan arvatusta salasanasta ja sitä kokeillaan kaapattuun kädenpuristukseen. Riippuen salasanan vahvuudesta murtaminen voi viedä hetken tai hyvin pitkän ajan. [12][42]

3.4. WPA2 – AES

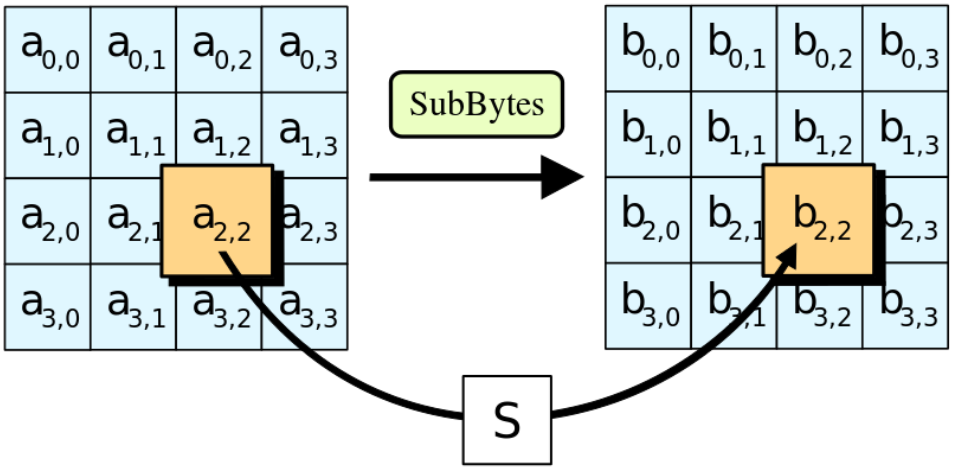
WPA2 perustuu IEEE 802.11i standardiin, joka esiteltiin 2004. Se on symmetrinen lohkosalaus, joka salaa ja purkaa dataa 128 bitin lohkoissa. Avainkokona voidaan käyttää 128, 192 ja 256 bittiä. Salaus AES:lla tapahtuu kierroksittain, joilla vaihdellaan ja korvataan salattavan paketin osia. Kierrosten määrä määräytyy avainkoon perusteella. 128-bitin avaimella kierroksia on 10. Jokaiselle kierrokselle johdetaan oma avain salausavaimesta. Jokainen kierros sisältää toimenpiteitä, jolla alkuperäinen data salataan. Kun data puretaan, toteutetaan salaustoimenpiteet päinvastaisessa järjestyksessä käyttäen samaa salausavainta. AES toteuttaa salauksen käyttämällä 4x4 bittimatriiseja. Varsinaiset kierrokset sisältävät neljä prosessointi askelta, joilla alkuperäinen data salataan. [5][33][36]



Kuva 16: AES salauksen vaiheet. [33]

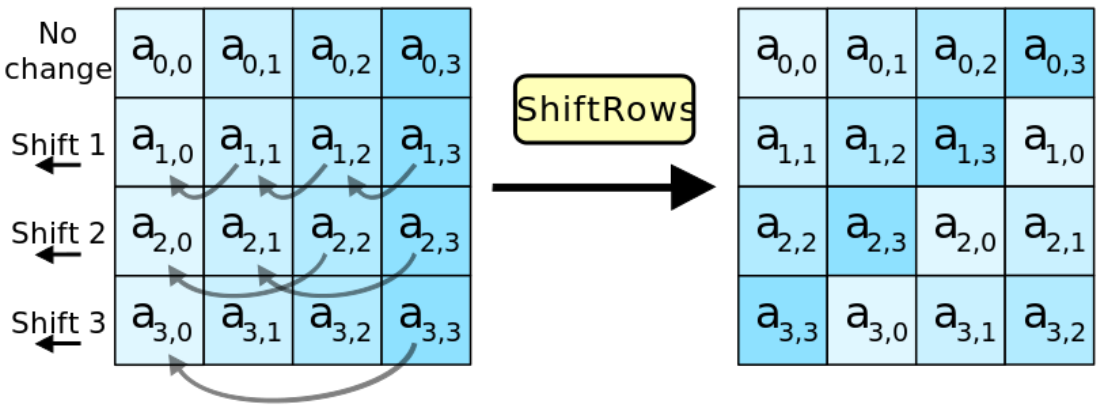
3.4.1 AES salauksen kierrosten vaiheet

Ensimmäinen vaihe salauksessa on bittien vaihto. jokainen bitti alkuperäisestä datasta vaihdetaan 8-bittisen vaihtolaatikon avulla, joka on nimeltään S-box. Bittien vaihto saa salauksessa aikaan epälineaarisuutta. Bittien vaihto tehdään niin, ettei siihen voi kohdistaa matemaattisin keinoin kohdistuvaa hyökkäystä. [5][33][36]



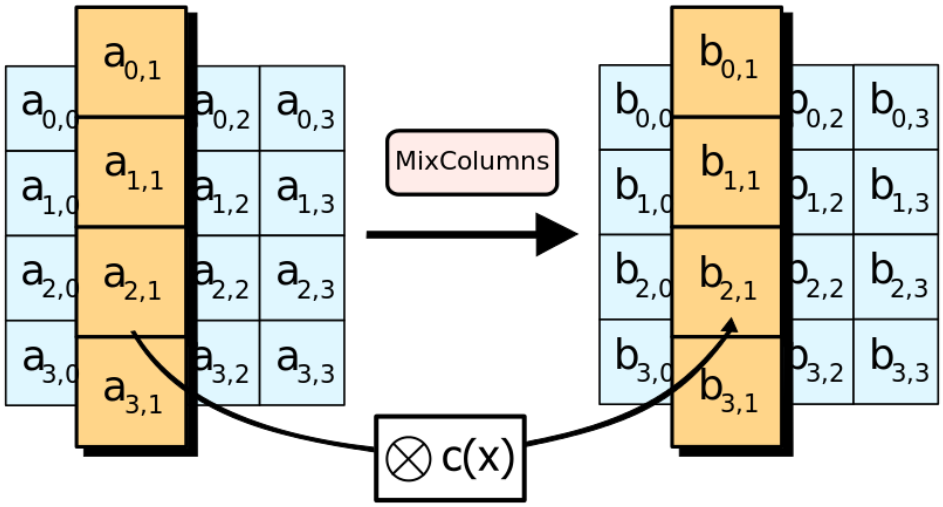
Kuva 17: Tavujen vaihto [5]

Toisessa vaiheessa laatikossa olevien bittien rivien paikkaa vaihdetaan. Ensimmäinen rivi pysyy paikallaan. Toista riviä siirretään yksi askel vasemmalle. Kolmatta riviä siirretään kaksi askelta vasemmalle ja neljättä riviä siirretään kolme askelta vasemmalle. [5][33][36]



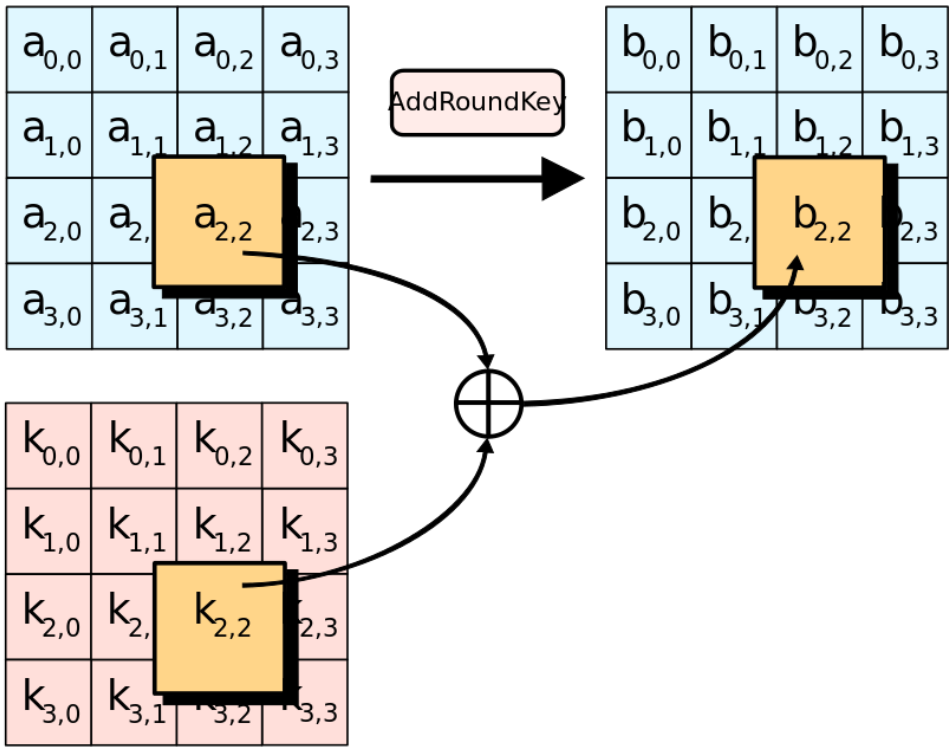
Kuva 18: Rivien vaihto [5]

Kolmannessa vaiheessa matriisin jokainen sarake muutetaan kertomalla se 4x4 matriisilla. [5][33][36]



Kuva 19: Sarakkeiden muuttaminen [5]

Neljännessä vaiheessa lisätään kierrosavain. Jokaiselle kierrokselle avain johdetaan erikseen pääavaimesta. Kierrosavaimet ovat yhtä suuria vaiheen kanssa. Kierrosavaimen jokainen bitti yhdistetään vaiheen bittien kanssa XOR:lla. [5][33][36]



Kuva 20: Kierrosavaimen lisääminen [5]

Neljä edellä mainittua vaihetta muodostavat yhden kierroksen. Kierroksia toistetaan avaimen pituudesta riippuen 9-13 kertaa. Viimeisellä kierroksella sarakkeiden muuttaminen jätetään tekemättä. Sarakkeiden muuttaminen jätetään tekemättä, koska se ei vahvista salausta kun se tehdään salauksen loppuun. Toisin sanoen sarakkeiden muuttaminen salauksen loppuun on turhaa. Purettaessa salausta, tehdään samat kierrokset ja niiden vaiheet käännetyssä järjestyksessä, kunnes salattu data on jälleen selkokielisenä. AES tarvitsee enemmän tilaa salauksen purkuun, kuin itse salausprosessiin. [5][33][36]

3.4.1 AES salaukseen kohdistuvat hyökkäykset

Vaikka AES on vahva salaus, voidaan sitäkin vastaan hyökätä. Vaikka itse pääavain on hyvin suojassa, koska sitä ei koskaan lähetetä ilmateitse laitteelta toiselle, voidaan siitä kaivaa tietoja sivukanavia pitkin. Tällaisia kanavia ovat salaamiseen kuluva aika, laitteen virrankulutus, laitteen elektromagneettinen kenttä prosessin aikana ja laitteen toiminta vian ilmentyessä. Sivukanavahyökkäykset keskittyvät siis salauksen fyysisiin ominaisuuksiin sen sijaan, että niillä pyrittäisiin vaikuttamaan itse salauksen haavoittuvuuksiin. Sivukanavahyökkäyksenä voi toimia salausaikaan kohdistuva hyökkäys. Se toteutetaan mittaamalla tarkkaan salaustoimenpiteisiin kuluva aika. Oletuksena on, että salaukseen kuluva aika on riippuvainen salausavaimen pituudesta. Myös laitteiston virrankulutusta voidaan analysoida salausprosessin aikana. Tätä kautta voidaan myös kerätä tietoa. Tarkoituksena on mitata välitöntä virrankulutusta, jota salaus aiheuttaa ja analysoida siinä tapahtuvia muutoksia. Edellä mainittuja asioita

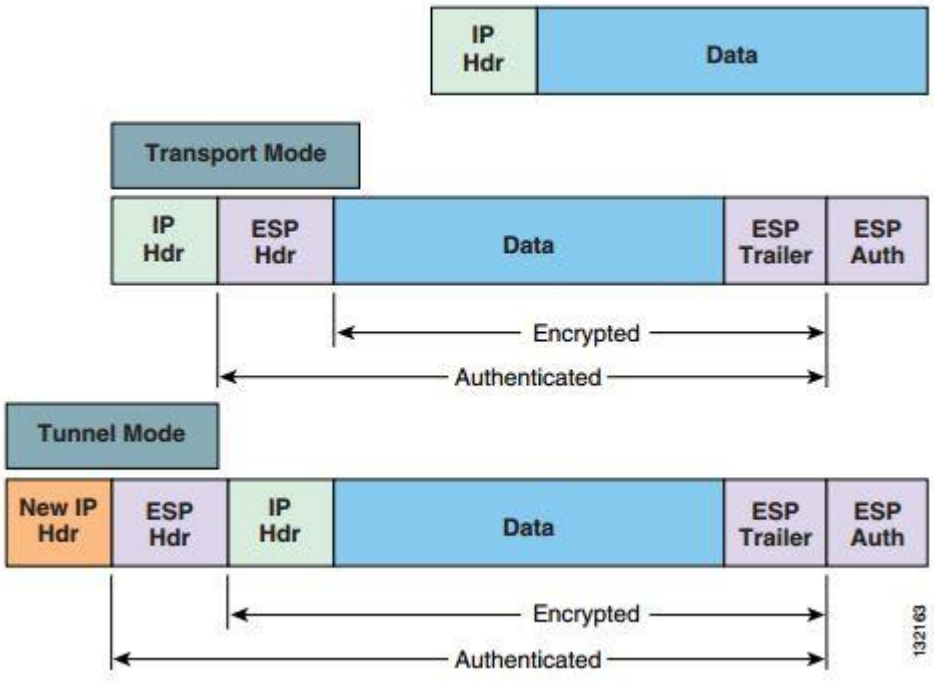
päästään analysoimaan välimuistin kautta, johon tarvittavia tietoja pääsee vuotamaan. Ongelmana tämän kaltaisissa hyökkäyksissä on se, että saadaan kaivettua tarpeeksi tarkkoja tietoja, jotta niistä voitaisiin tehdä järkeviä päätelmiä salaukseen liittyen. Sivukanaviin kohdistuvat hyökkäykset voivat tapauskohtaisesti kestää muutamasta sekunnista useisiin tunteihin. [7][14][11][34]

3.5. VPN

VPN-yhteydet on kehitetty suojaamaan tiedonsiirtoa pisteiden välillä, jossa muuten ei olisi suojattua yhteyttä. Yleisimmin käytössä oleva protokolla on IPsec. VPN yhteyksiä käytetään yleensä etäyhteyksien muodostamiseen internetin yli. Tällä tavoin työntekijöiden on mahdollista olla yhteydessä työasemiinsa kotoa kannettavalla tietokoneella tai mobiililaitteella. VPN-yhteyksillä voidaan myös yhdistää yritysten sisäisiä verkkoja toisiinsa, jolloin eri paikoissa olevista toimipisteistä on mahdollisuus olla yhteydessä samaan sisäiseen verkkoon. VPN muodostaa verkon läpi kaksi tunnelia, joista toista käytetään avainten vaihtoon, ja toista datan siirtoon. Langattoman verkon kanssa käytössä on yleensä IPsec-protokolla, jonka avulla liikkuva data salataan, tunnistetaan ja sen eheys tarkistetaan. Jokaiselle lähtevälle datapaketille luodaan oma sormenjälki, jota ei voida väärentää. Sen avulla voidaan päätellä, onko siirrettävää dataa käpälöity lähetyksen ja vastaanoton välissä. Paketit, joita ei tunnisteta hylätään, eikä niitä toimiteta vastaanottajalle. Salauksesta ja tunnistuksesta vastaa ESP -protokolla. Se käyttää salaukseen haluttua salausalgoritmia, kuten AES:ia. Se voi myös suorittaa tunnistuksen, mutta se ei kuitenkaan salaa omaa ESP -tunnistustaan. [19][24][38]

Tunnistusotsikko (AH) vastaa datan tunnistamisesta. Se käyttää samaa algoritmia kuin ESP. Se tarjoaa myös suojaa datapakettien luvattomien uudelleenlähetysten varalle. Tunnistusotsikko sijoitetaan IP-otsikon ja varsinaisen datan väliin kehyksessä. tunnistusotsikko suojaa datapaketin alkuperän ja määränpään, muttei vastaa datan luottamuksellisuudesta. Mikäli datapaketti siepataan ja käytössä on vain tunnistusotsikko, voidaan datan sisältö lukea. [19][24][38]

VPN yhteys voi toimia kahdella eri tavalla. Käytössä voi olla joko siirtomoodi tai tunnelimoodi. Siirtomoodissa ainoastaan kehyksen hyötydata on salattu, eikä IP otsikkoa muuteta. Siirtomoodissa liikkuvan datan alkuperä ja määränpää ovat alttiina tiedustelulle. Hyökkääjä saa helposti IP otsikosta nämä tiedot, koska sitä ei ole salattu. Tunnelimoodissa koko paketti IP otsikkoa myöten käsitellään ja siihen liitetään uusi IP otsikko, jossa on kaksi IPsecin osoitetta. Näissä osoitteissa tapahtuu paketin salaus ja purku. Tunnelimoodissa hyökkääjä ei pääse analysoimaan lähetettävää dataa, eikä saa selville mistä tai minne data on menossa. [19][24][38]



Kuva 21: VPN kehykset eri moodeissa [24]

Avaintenhallinta tapahtuu VPN -yhteydessä IKE-protokollan avulla. Se asettaa ja vaihtaa avaimet automaattisesti osapuolten välillä. Avainten käytöllä varmistetaan, että ainoastaan viestin lähettäjä ja vastaanottaja pystyvät lukemaan sen. IKE vaatii, että avaimet luodaan uudestaan tai päivitetään vähän väliä, jotta yhteys pysyy turvallisena. Käyttäjä voi itse määrittää avaimen vahvuuden ja päivitysvälin. IKE-protokollassa on kaksi moodia, jota voidaan käyttää: päämoodi ja aggressiivinen moodi. Päämoodissa lähetetään kolme viestiparia, joilla määritetään salausalgoritmi, eheydensuojausalgoritmi, tunnistusmenetelmä ja niin sanottu Diffie-Hellman -ryhmä. Aggressiivisessa moodissa lähetetään vain kolme viestiä, joilla hoidetaan samat asiat. Aggressiivisessa moodissa voidaan myös käyttää ennalta määritettyä salausavainta. Aggressiivisen moodin hyvä puoli on sen nopea yhteydenmuodostus, mutta varjopuolena

on turvattomuus. Sen ensimmäistä viestiä ei ole salattu, ja se voidaan kaapata. Siitä voidaan päätellä keskustelun osapuolet ja mahdollisesti murtaa ennalta määritetty salasana. Tämä voi johtaa man in the middle hyökkäyksen mahdollisuuteen, jolloin kaikki liikenne kulkee kolmannen osapuolen kautta lähettäjän ja vastaanottajan tietämättä. Pääosin VPN-yhteyttä pidetään hyvin luotettavana ja sitä käytetään, kun halutaan siirtää luokiteltua tietoa kahden pisteen välillä. [19][24][38]

4. LANGATTOMAAN VERKKOON KOHDISTUVAT UHKAT MAANTIETUKIKOHTAYMPÄRISTÖSSÄ

Tässä use case -tutkimuksessa on tarkoitus tutkia maantietukikohtaympäristössä oleviin langattomiin verkkoihin kohdistuvaa uhkaa. Uhkaa pohditaan hyökkääjän näkökulmasta ja esille tuodaan asioita, jotka vaikuttavat hänen toimintaansa. Pohdittaessa vaikutusmahdollisuuksia otetaan huomioon, että mahdollinen toimija on yksin tai korkeintaan pienessä ryhmässä toimiva kokonaisuus. Maantietukikohtaan ei siis kohdisteta jonkin tietyn maan tiedustelun koko voimaa. Tukikohtaa puolustavien joukkojen määrään tai sijoitteluun ei oteta kantaa, jotta tutkimuksen turvaluokka pysyy julkisena. Tästä johtuen osio sisältää hyvin paljon omaa pohdintaa, sillä asiakirjojen lähteenä käyttö hankaloituu turvaluokituksen takia. Esimerkkitukikohdaksi valitsen Joutsan varalaskupaikan, johon on mahdollista perustaa maantietukikohta. Otan käsittelyyn kolme erilaista tapausta, jotka sijoittuvat rauhanajan harjoitukseen, kiristyneeseen tilanteeseen ja sotatilaan. Jokaisessa tapauksessa pohdin erikseen, millaisia uhkia tukikohtaan voidaan kohdistaa ja toisaalta kuinka helppoa ja hyödyllistä kyseisen uhkan luominen hyökkääjälle on.

Maantietukikohdan tarkoitus on luoda tukeutumisedellytykset hävittäjäkalustolle sodan aikana. Maantietukikohtaan luodaan samankaltaiset tukeutumisedellytykset kuin päätukikohtiin, joskin tilat ovat hieman alkeellisemmat ja koostuvat lähinnä konteista ja muusta siirrettävästä kalustosta. Maantietukikohtia voidaan käyttää niin rauhanajan harjoitteluun, kuin sotatilassa toimimiseen. Maantietukikohtien suojaamiselle luo haasteita niiden sijainti. Esimerkkinä käytettävä Joutsan varalaskupaikka sijaitsee nelostiellä aivan Joutsan kylän vieressä. Sen lisäksi, että varalaskupaikan läheisyydessä on runsasta siviiliasutusta, on nelostie myös yksi suomen vilkkaimmin liikennöidyistä.

Ennen kuin valmiuslaki tai puolustustilalaki astuu voimaan, puolustusvoimilla on rajalliset mahdollisuudet ihmisten liikkumisen rajoittamiseen ja erilaisiin vastatoimiin. Mikäli maantietukikohta on tarpeellista ottaa käyttöön jo siinä vaiheessa, kun puhutaan normaalioloista, on sen suojaaminen haasteellista. Käytännössä suojaustoimet edellyttävät aina yhteistyötä poliisin kanssa. Kun maantietukikohta otetaan käyttöön katkaistaan liikenne sitä kautta kulkevalta tieltä ja se ohjataan kiertoreitille. Ihmisiä varsinaisen nousutien varresta evakuoidaan tilanteesta riippuen. Rauhan aikana ketään ei välttämättä siirretä tieltä pois, sillä ainoastaan nousutie ja monesti sen välittömässä läheisyydessä olevat koneiden kääntöpaikat ovat ainoa alue joka eristetään. Mahdollisen hyökkääjän kannalta tilanne taas on tilanteesta riippuen joko hyvin helppo tai haastava. Yksi asia, joka kuitenkin yhdistää jokaista tuleva tapausta, on se, että

varalaskupaikkojen sijainti on etukäteen tiedossa oleva asia. Tästä johtuen niiden ympäristö on mahdollista tiedustella hyvissä ajoin ennen kuin jokin konflikti uhkaa. Uusien varalaskupaikkojen luominen yhtäkkiä salassa ei onnistu, sillä mikä tahansa valtatien remontointi herättää monesti huomiota ja nousutie tarvitsee aina leveämmän väylän kuin normaali maantie. [37]

Kuva 23: Joutsan varalaskupaikka, nousutie ympyröity punaisella [18]

4.1. Uhkat rauhanajan harjoituksien aikana.

Rauhan aikana suoritetuissa harjoituksista uutisoidaan hyvissä ajoin ja tukikohta-alueen lähelle pääsee siviilihenkilöitä. Siviilien kulkua on vaikea kieltää jo senkin vuoksi, että maantietukikohta sulkee paljon tiestöä ja sen varrella asuu paljon paikallista väestöä. Paikallisille on järjestettävä kulku koteihinsa. Monesti yleisölle järjestetään myös mahdollisuus seurata lentotoimintaa sen ollessa käynnissä. Ympäröivän väestön elämää ei siis haluta turhaan hankaloittaa. Näin ollen vartiointi toteutetaan siten, etteivät ihmiset pääse pyörimään mahdollisten lentokoneiden tai muun kaluston ympärille ja aiheuttamaan vaaraa käytettävillä nousu- ja rullausteillä. Vartioinnista vastaavat yleensä sotilaspoliisit, joilla ei ole merkittävästi toimivaltaa siviiliväestöä kohtaan, elleivät he tuota suoranaista uhkaa tukikohdassa tapahtuvaa toimintaa kohtaan. Alueen läheisyydessä pyörii siis runsaasti paikallisia ihmisiä ja sen lisäksi mahdollisesti uteliaita turisteja, jotka ovat halunneet tulla seuraamaan toimintaa. Näiden ihmisten sekaan voi helposti sulautua joku, joka haluaa kohdistaa maantietukikohtaa kohtaan jonkin sortin vihamielisyyksiä. Rauhanajan harjoituksissa ei myöskään välttämättä ole riittävästi henkilöstöä, joka ehtisi seuraamaan tarkemmin ympäröivien siviilien toimintaa ja käyttäytymistä tukikohdan läheisyydessä. [37]

Mahdollinen hyökkääjä pääsee haluamalleen paikalle melko helposti, sillä kulkua on yleisesti pyritty rajoittamaan mahdollisimman vähän tukikohdan ympärillä. Myös mahdolliset hyökkäyspaikat on helppo tiedustella etukäteen, koska harjoituksesta on todennäköisesti ollut tieto jo varhaisessa vaiheessa. Kun hyökkääjä on siirtynyt haluamaansa paikkaan, voi hän rauhassa suorittaa haluamaansa kohteeseen toimenpiteitä. Rauhanajan harjoituksessa viestiyhteydet ja välineet eivät välttämättä ole täysin mitoitettuja tositilanteeseen, sillä monesti niissä harjoitellaan yksinomaan lentotoimintaa. Joka tapauksessa mahdollinen hyökkääjä kykenee melko vaivattomasti suorittamaan esimerkiksi passiivista kuuntelua alueen langattomista verkoista. Mikäli hän löytää jonkin mielenkiintoisen verkon, voi hän yrittää murtautua sen sisälle tai suorittaa palvelunestohyökkäyksen. Rauhanaikana järjestelmien toimimattomuuteen ei välttämättä käydä käsiksi kiireellä, ellei järjestelmä ole kriittinen esimerkiksi lentoturvallisuuden kannalta. Jos hyökkääjä ei toimi aggressiivisesti, voivat hänen toimet jäädä helposti huomaamatta. Kauempaa toimiessa tarvitaan suurempia antenneja, joiden käyttäminen voi herättää kiinnostusta tukikohdan joukoissa ja alueella asuvissa siviileissä. Rauhan aikana hyökkääjän ei kuitenkaan tarvitse toimia pitkien etäisyyksien päästä. Mahdollinen hyökkääjä pyrkii toimimaan mahdollisimman huomaamattomasti ja hänen käytössään voi olla toimintaan sopivaksi muokattu ajoneuvo.

Yksi keino päästä lähelle maantietukikohtia, on ostaa niiden läheisyydestä esimerkiksi maatila, johon voi rakentaa laillisesti antenneja ja muita laitteita, joilla perustettavan tukikohdan suuntaan voi toimia. Varsinkaan rauhan aikana omalla maalla tapahtuvaa toimintaa ei pystytä estämään. Tässä työssä ei kuitenkaan ole tarkoitus ottaa kantaa mahdollisiin maakauppoihin ilmavoimien kohteiden läheisyydessä.

Harjoitukset kestävät monesti viikon tai kaksi, joten sinä aikana ehtii tekemään paljon. Kuten aikaisemmissa luvuissa on käynyt ilmi, nykyaikaisiin verkkoihin ei välttämättä pääse murtautumaan brute force menetelmällä, vaikka käytössä olisikin kaksi viikkoa. Tämä ei kuitenkaan poista sitä mahdollisuutta, että verkkoja kuunnellaan ja niistä kerätään mahdollisimman paljon informaatiota analysoitavaksi ja myöhemmin käytettäväksi. Lisäksi hyökkääjä voi palvelunestohyökkäyksellä testata reaktioita ja reaktioaikoja tapahtumiin. Halutessaan hyökkääjä voi myös testata hieman näkyvämpää toimintaa ja sitä, millä tavoin tukikohdassa reagoidaan ympärillä liikkuviin kulkijoihin. Rauhan ajan harjoituksen yhteydessä tämä ei kuitenkaan ole välttämättä järkevää. Pääasiassa hyökkääjän toiminnan tarkoitus rauhan aikana on suurimmaksi osaksi tiedustelua. Mikäli hyökkääjä jää kiinni, ei hänellä ole minkäänlaisia yhteyksiä valtiollisiin toimijoihin, vaan hän jää kiinni yksityishenkilönä. Tällöin hänen toiminta ei aiheuta poliittisia jännitteitä tai virallisia epäilyjä.

Sen lisäksi, että hyökkääjä voi kohdistaa toimiaan tukikohdan järjestelmiin, voi hän myös ottaa kohteekseen yksittäiset sotilaat alueella. Nykyään kaikilla on mukanaan jonkinlainen langaton laite, jota käytetään päivittäin. Mikäli tällaiseen laitteeseen päästään murtautumaan, voidaan sen avulla hankkia arvokasta lisätietoa tukikohdan toimijoista. Esimerkiksi puhelimen tai muun multimedialaitteen salakuuntelu voi antaa hyökkääjälle paljon tietoa, jonka hankkiminen muuten voisi olla lähes mahdotonta. Tämä pätee tietenkin muuallakin tapahtuvaan toimintaan, kuin pelkkään maantietukikohtaan. Varsinkin rauhan aikana ihmiset saattavat toimia varomattomasti omien kannettavien tietokoneiden, älypuhelinten ja tablettien kanssa. Rauhan ajan toiminnassa älylaitteita ei saa käyttää tietyn turvaluokan ylittävissä tiloissa, mutta laitteita ei silti kerätä pois joukoilta, mikä saattaa johtaa inhimillisiin unohduksiin. Toinen asia voi olla välinpitämättömyys. Ei välttämättä uskota, että joku voisi päästä käsiksi omaan älylaitteeseen. Mikäli yksittäiseltä henkilöltä saadaan varastettua yksityisiä tietoja, voidaan niitä käyttää myöhemmissä tilanteissa kiristykseen ja painostamiseen. Yksittäiseen henkilöön kohdistuva tiedustelu kattaa myös sosiaalisen median ja muun toiminnan internetissä. Tukikohdassa toimivista joukoista voi helposti saada käsityksen sosiaalisen median välityksellä. Monet tiedot, jotka ladataan sosiaaliseen mediaan, voivat paljastaa tukikohdassa toimivia henkilöitä ja sitä, mitä he ovat siellä tekemässä. Henkilöstöön kohdistuvan tiedustelu ei

siis välttämättä vaadi paikan päällä oloa tai langatonta verkkoa, jotta sitä voidaan toteuttaa. [20]

Rauhan aikana suoritettu toiminta maantietukikohtaa vastaan on siis todennäköisesti hyvin tiedustelupainotteista. Hyökkääjän päätehtävänä on pääasiassa hankkia tietoa tukikohdan verkkorakenteesta, yhteyspisteistä ja verkon käytöstä. Toisena tehtävänä on todennäköisesti tukikohdan ympäristön tiedustelu, jotta kriisi- ja sotatilanteessa toimiminen olisi helpompaa. Hyökkääjän harjoittamaa passiivista kuuntelua ei voida havaita, joten siihen on mahdoton puuttua muuten kuin kiinnittämällä huomiota omaan toimintaan. Kaiken kaikkiaan rauhanajan ympäristö tarjoaa hyökkääjälle helpot puitteet suunnittelulle ja tiedustelutoiminnalle. Mikäli rauhan aikana suoritetulla verkkojen kuuntelulla saadaan selville verkon laitteistoa ja suojausmenetelmiä, voidaan niiden varalle suunnitella toimenpiteitä jatkoa ajatellen. Rauhan aikana suoritettu toiminta langattomia verkkoja kohtaan tähtää kuitenkin siihen, että jos joskus tilanne kiristyisi, olisi toiminnan aloittaminen silloin helppoa. Tilanteen kiristyessä ei tarvitsisi aloittaa tiedustelua alusta, vaan tietyt perusasiat olisivat jo tiedossa, jonka pohjalta toiminnan saisi nopeasti käyntiin. On kuitenkin muistettava, että yksittäiset maantietukikohdasta suoritettavat harjoitukset eivät välttämättä kiinnosta suuria valtiollisia toimijoita niin paljoa, että niihin kohdistuisi joka kerta tietoturvauhka. Toki verkkoihin kohdistuvaa salakuuntelua ja murtautumisyrityksiä voi tehdä myös puhtaasti siviilihenkilöt oman harrastuneisuuden vuoksi, mutta näkisin sen hyvin epätodennäköisenä.

4.2. Uhkat kiristyneessä tilanteessa.

Kiristyneessä tilanteessa toimiminen vaatii hyökkääjältä enemmän varovaisuutta, kuin rauhan aikana. Hyökkääjä on mitä todennäköisemmin jonkinlainen erikoisjoukkosotilas, jolloin voidaan olettaa, että hänen taitotasonsa välttää vastapuolen vartioiden partioita tukikohdan ulompien kehien sisällä on kohtalainen. Mikäli hyökkääjä on suunnitellut toimintansa hyvin, on hän voinut toimittaa alueelle haluamansa laitteet jo hyvissä ajoin rauhan aikana ja virittää omasta mielestään keskeisiin sijainteihin antenneja ja muita laitteita. Kun tilanne on kiristynyt, kiinnitetään alueen läheisyydessä toimiviin ja oleileviin ihmisiin huomattavasti suurempaa kiinnostusta, joten kaikenlainen epäilyttävä liikehdintä herättää huomiota. Tämän vuoksi hyökkääjällä ei myöskään ole samanlaista liikkumisen vapautta, kuten rauhan aikana, vaan hän joutuu hyvin todennäköisesti toimimaan kauempaa. Tässä tilanteessa ennalta suoritettu alueen maastonkartoitus astuu tärkeään rooliin. Kriisistä riippuen alueella saattaa kuitenkin asua vielä siviiliväestöä, joka vaikeuttaa tukikohdan joukkojen toimintaa mahdollisen hyökkääjän suhteen.

Samalla kun siirrytään lähemmäs sodan aikaa, lisääntyy myös tukikohdassa olevien viestijärjestelmien määrä. Kun varsinaista maantietukikohtaa aletaan rakentamaan, on hyökkääjälle tärkeää tiedustella missä tukikohdan viestijärjestelmät sijaitsevat, jotta niihin olisi mahdollista vaikuttaa. Kun tukikohta on rakennettu, ei sen kokoonpanoa muuteta tiuhaan. Tämä johtuu jo siitä seikasta, että maantietukikohdan alue on kohtalaisen pieni. Pääosa maantietukikohtaan rakennettavasta infrastruktuurista keskittyy kiitotien läheisyyteen, joka on paikasta riippuen kilometristä kahteen pitkä. Kokoonpano on näin ollen melko helppo tiedustella, mikäli käytössä on oikeanlaista laitteistoa. Verkkotiedusteluun sopivien laitteiden hankkiminen ei ole nykyään kovinkaan hankalaa, varsinkin jos kyseessä on jokin valtiollinen toimija. Verkkokortit ja antennit eivät myöskään ole kovinkaan kalliita.

Kun tukikohtaa rakennetaan, hyökkääjällä on mahdollisuus hankkia yhä enemmän tietoa kuuntelemistaan järjestelmistä. Rakennusvaiheessa alue ei vielä ole täysin miehitetty ja toiminnassa voi esiintyä huolimattomuutta. Mikäli vartiointia ei ole järjestetty kunnolla, voi hyökkääjä yrittää päästä tukikohta-alueen sisäpuolelle, mutta siihen sisältyy aina kiinnijäämisen riski. Lisäksi kerran epäilyttäväksi todettua henkilöä pidetään varmasti tarkemmin silmällä, kuin sellaista, joka ei ole aiheuttanut ongelmia. Kiristyneessä tilanteessa omaa toimintaa ei välttämättä kannata paljastaa suorittamalla aktiivisia toimia alueella, mikäli toimintaa on tarkoitus jatkaa vielä, kun sota syttyy. Kiristyneessä tilanteessa suoritettava mahdollinen hyökkäys tukikohdan järjestelmiin ei tapahdu yksinään, vaan sillä on yhteys johonkin isompaan

tapahtumaan. Hyökkääjä haluaa joko harhauttaa ja sitä kautta suojata muualla tapahtuvaa toimintaa, tai tehostaa jonkin toisen tapahtuman vaikutusta tukikohtaa vastaan. Tallaisessa tilanteessa mahdollisia toimia ovat palvelunestohyökkäys ja verkkojen häirintä. Näillä toimilla pyritään vaikeuttamaan tukikohdan toimintaa. On myös hyvin oletettavaa, että samankaltaista toimintaa kohdistetaan samanaikaisesti muidenkin maantietukikohtien läheisyyteen, mikäli niitä on rakenteilla. Mikäli tukikohtaa vastaan suunnataan aktiivisia toimia, paljastuvat ne hyvin nopeasti, jolloin tukikohdassa voidaan ryhtyä vastatoimiin. Tällaisessa tilanteessa toiminnan jatkaminen voi olla mahdotonta, mutta hyökkääjällä on voinut olla tehtävänään toimia vain kriisitilanteen alkuun asti ja poistua sen jälkeen alueelta.

Varsinaisen maantietukikohdan ympärillä olevaa aluetta ei välttämättä kriisin alkuvaiheessa vartioida kovinkaan raskaasti, koska alue sijaitsee syvällä sisämaassa. Oletettavasti alueet, joilla puolustusvoimat toimivat ovat tässä vaiheessa eristettyjä, mutta esimerkiksi Joutsan kaupunkia ei välttämättä ole vielä tyhjennetty. Tilanteesta riippuen sitä voi käyttää hyvänä tukipisteenä ja kaupungissa sijaitsevia mastoja ja korkeita rakennuksia apuna, kun yritetään muodostaa näköyhteyttä tukikohta-alueelle.

Yhteenvetona voidaan todeta, että kriisitilanteessa, jolloin käytössä voi olla jo puolustusvoimien toimintaa helpottavia lakeja, tukikohtaa vastaan toimivan hyökkääjän toiminnanvapaus rajoittuu. Maantietukikohtaa rakennettaessa, sen sisältämät järjestelmät lisääntyvät, jolloin hyökkääjän tiedusteltavissa olevien laitteiden ja yhteyksien määrä lisääntyy. Paikallisen siviiliväestön määrä vaikuttaa suoraan hyökkääjän toimintaan. Mitä enemmän siviilejä alueen läheisyydessä liikkuu, sitä helpompi niiden sekaan on sulautua. Toisaalta pienellä paikkakunnalla liikkuvat ulkopuoliset henkilöt voivat herättää epäilyksiä paikallisissa, jotka saattavat raportoida näkemyksiään maantietukikohdan joukoille. Kaikin puolin hyökkääjän on siis toimittava huomattavasti varovaisemmin, mutta samalla hänen käsillään oleva tiedon määrä kasvaa. Kriisin alkuvaiheessa maantietukikohtaa vastaan kohdistuva toiminta on edelleen suurelta osin tiedustelua, jonka pohjalta saatetaan myöhemmin aloittaa aktiivisempia toimenpiteitä.

4.3. Uhkat sodan aikana.

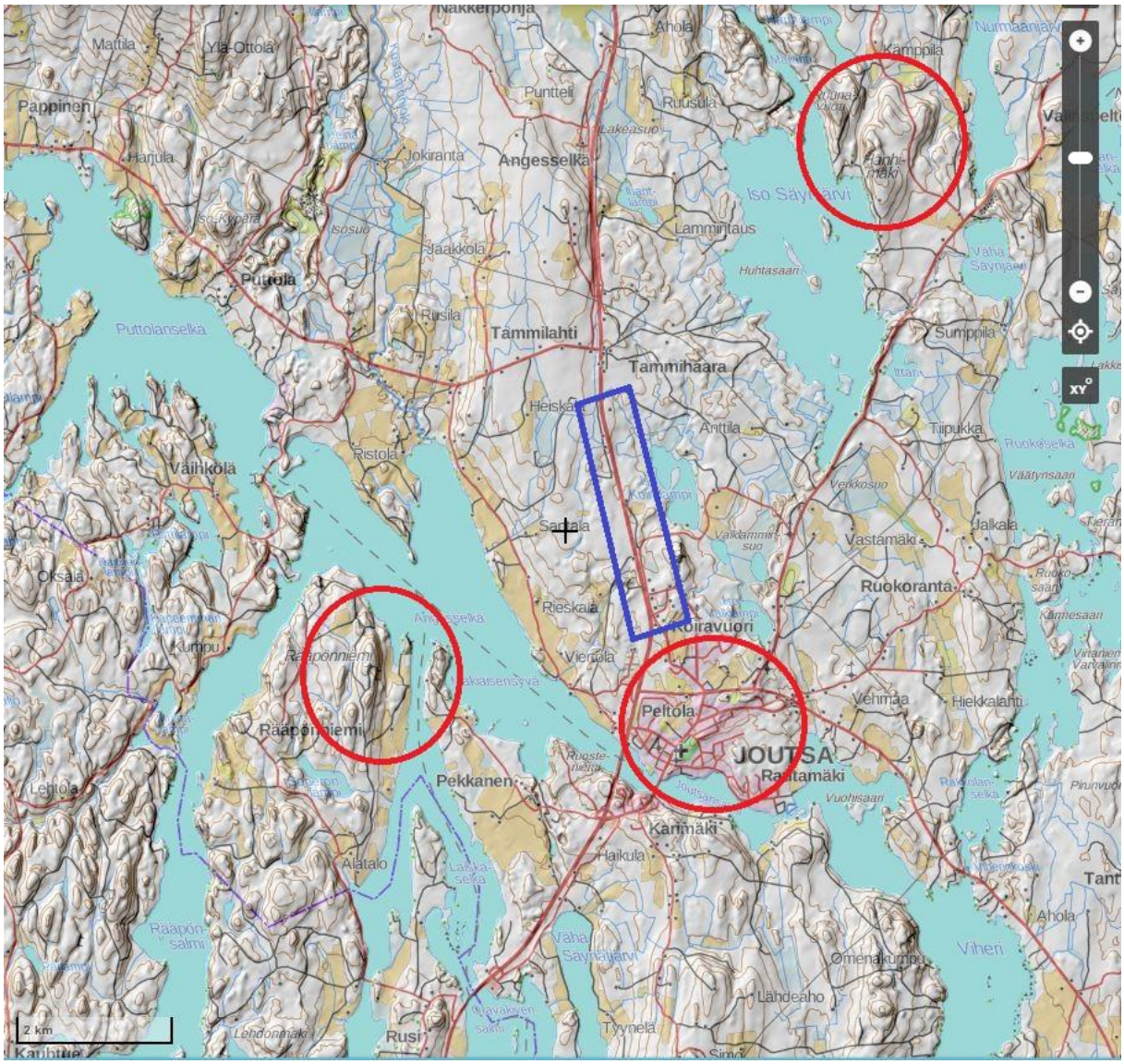
Sodan aikana tukikohdan suojauskehät ulottuvat pisimmälle, joten hyökkääjän voi olla vaikea päästä riittävän lähelle, jotta mahdollisuudet vaikuttamiselle olisivat olemassa. Sodan aikana alueella ei liiku enää siviilejä, joten jokainen tukikohdan ulkopuolinen kulkija alueella herättää huomiota. Toiminta on pidettävä huomattavan matalalla profiililla ja aktiiviset toimet on yhdistettävä tukikohtaan kohdistuviin mahdollisiin muihin uhkiin, jolloin oma kiinnijääntі on epätodennäköisempää. Tällaisessa tilanteessa kiinni jäämisen jälkeen ei ole enää epäselvää, etteikö maantietukikohtaa vastaan toimiva henkilö liittyisi suoraan sotatoimiin.

Sodan aikana kriittisten järjestelmien kaataminen tai häirintä voi olla ratkaisevaa oikealla hetkellä. Tässä vaiheessa rauhan aikana ja kiristyneessä tilanteessa kerätystä ja tiedustellusta datasta voi olla hyötyä, mikäli se on voitu analysoida huolella. Alueella toimiva hyökkääjä on todennäköisesti useampaan otteeseen yhteydessä omiin joukkoihinsa, jotta oikea-aikaiset hyökkäykset olisivat mahdollisia.

Kaiken kaikkiaan maantietukikohtaan kohdistuvan uhkan kulku on todennäköisesti sellainen, että rauhan aikana keskitytään enemmän tiedusteluun ja verkkojen kuunteluun. Kun tilanne alkaa kiristyä, aletaan verkoista saatua tietoa käyttämään hyväksi hyökkäysten suunnittelussa. Hyökkäys toteutetaan kriittisellä hetkellä, jolloin sillä saadaan aikaan suurin vaikutus. Verkkohyökkäyksellä ei yksinään ole suurta merkitystä tukikohdan toiminnalle, mutta mikäli se liitetään osaksi suurempaa kokonaisuutta, voidaan saada aikaan merkittävää lisävaikutusta.

Hyökkääjällä tulee olla näköyhteys kohteeseensa, jotta langattomien verkkojen taajuusalueelle saadaan yhteys pitemmän matkan päästä. Lisäksi hyökkääjä tarvitsee käyttöönsä suuren antennivahvistuksen omaavia antenneja, jotta muuten heikko vastaanotettava signaali olisi mahdollista kuulla. Ei ole realistista olettaa, että hyökkääjällä olisi mahdollisuus päästä tukikohdan sisälle verkkolaitteiden läheisyyteen, joten toiminta kauempaa on ainut vaihtoehto. Tukikohdan ympäristöstä voi kuitenkin helposti löytyä toiminnalle sopiva paikka. Kiitotiet vaativat kohtalaisen suuren tasaisen alueen ympärilleen, jolloin kauempana olevat maastonmuodot voivat mahdollistaa näköyhteyden muodostamisen. Tukikohdat sijaitsevat lisäksi sisämaassa, joten niiden ympäristössä ei välttämättä ole suurta puolustavaa voimaa, joka aktiivisesti etsisi yksittäisiä erikoisjoukkosotilaita alueelta. Lisäksi pienissä kokoonpanoissa tapahtuvaa toimintaa on hyvin vaikeaa havaita, vaikka alueella toimisikin puolustavia joukkoja.

Nopeasti analysoimalla Joutsan maastokarttaa voidaan huomata, että itse kiitotein alue on hyvinkin tasaista, mutta sen läheisyydessä on järvien molemmin puolin korkeita maastonkohtia, jotka voivat sopia hyvin hyökkääjälle. Lisäksi Joutsan keskustasta voi löytyä paikkoja, joita hyökkääjä voi käyttää hyväkseen.



Kuva 24: Joutsan maastokartta. Punaisella ympyröitynä hyökkääjän kannalta edulliset paikat [25]

Ylläolevasta kartasta on ympyröity sinisellä värillä kiitotien alue ja punaisella ne paikat, josta hyökkääjällä olisi mahdollisuus vaikuttaa. Parhaita paikkoja ovat Rääpönniemessä ja Hanhimäessä sijaitsevat korkeat maastonkohdat, joista on edellytykset toimia kenttää kohti. Joutsan kylällä voi myös olla yksittäisiä rakennuksia, joista voidaan toimia kenttää kohti. Joutsan kylä sijaitsee todella lähellä kiitotietä, mutta asutuskeskuksesta voi olla vaikea löytää yksittäisiä taistelijoita. Kaukaa korkeista maastonkohdista toimittaessa hyökkääjän on käytettävä antennia, jossa on suuri antennivahvistus. Tämä tarkoittaa sitä, että antennin koko kasvaa ja se voi

olla puolustavalle osapuolelle helpompi havaita. Suuren antennin liikuttaminen voi myös olla vaikeaa. Muutoinkin karttaa analysoimalla voidaan huomata, että vesistöt rajoittavat tukikohdan joukkojen ja infrastruktuurin sijoittelua. Samalla vesistöt helpottavat alueen vartiointia, mutta luovat suuria tasaisia alueita, jotka helpottavat signaalien kuuntelua. Puolustavan joukon kannalta parasta olisi, jos tukikohdan alueella olisi maastonmuotoja, joiden väliin langattomia linkkijänteitä voitaisiin rakentaa, jolloin niiden salakuuntelu vaatisi hyökkääjältä paljon enemmän vaivaa.

Yhteenvetona sodan aikana maantietukikohtaan kohdistuvasta uhkasta voi sanoa, että hyökkääjän toiminta vaikeutuu entisestään, kun siviiliväestö poistuu alueelta. Aikaisemmassa vaiheessa pystytetyillä järjestelmillä hyökkääjä voi jatkaa tiedustelua, mikäli niitä ei ole puolustavan organisaation toimesta havaittu. Tiedustelun lisäksi sodanaikana on erittäin todennäköistä, että tukikohtaa vastaan kohdistetaan joitain aktiivisia toimia. Aktiiviset toimet liittyvät hyvin todennäköisesti suurempaan kokonaisuuteen, jolla pyritään maksimoimaan tukikohtaa vastaan kohdistuva vaikutus.

5. JOHTOPÄÄTÖKSET

5.1. Langattoman verkon ominaisuudet ja uhkat

Langattomat verkot ovat viimeisen kahdenkymmenen vuoden aikana kehittyneet nopeiksi ja toimiviksi järjestelmiksi. Ne ovat omiaan toimimaan liikkuvassa toimintaympäristössä, jossa tarvitaan joustavuutta. Alun perin verkot olivat liian hitaita suurempien yritysten tai tahojen käyttöön, mutta nykyään nopeudet ovat niin suuria, että myös puolustusvoimien kaltaiset suuret toimijat pystyvät käyttämään niitä hyväkseen. Langallisiin verkkoihin verrattuna langattomuus tuo liikkumavaraa ja vähentää eri paikkojen väliin vedettävien kaapelien määrää. Tietyllä tapaa tämä lisää taistelunkestävyyttä, kun ei enää tarvitse pelätä, että jokin kaapeli menee poikki. Varjopuolena on se, että langattomat tiedonsiirtoyhteydet eivät kulje vain kahden pisteen välillä, vaan radiosignaalin ominaisuuksien vuoksi ne matkustavat vapaasti ilmakehässä. Antennivalinnoilla voidaan vaikuttaa siihen, kuinka laajalle alueelle säteilyä leviää. Vaikka käytetään suuntaavia antenneja, eivät ne silti poista sitä riskiä, että joku voisi kaapata signaalin ilmasta. Suuntaavat antennit säteilevät myös joka suuntaan, mutta niiden pääkeila voidaan ohjata oman toiminnan kannalta edulliseen suuntaan. Tukikohtakäytössä tämä on erityisesti huomioitavaa, sillä viholliset toimijat yrittävät varmasti mielellään päästä käsiksi tukikohdan sisällä kulkevaan dataan. Langattoman verkon taajuusalueessa on se hyvä puoli, että toimiakseen se vaatii käytännössä näköyhteyden. Toki myös langattomat signaalit heijastuvat pinnoista, mutta ne myös vaimenevat nopeasti.

Langattoman verkkotekniikan kehittyessä on huomioitavaa, että myös verkon suojausta on pitänyt kehittää. Alun perin yhteydet eivät olleet juuri millään lailla suojattuja ja niihin oli hyvinkin helppo murtautua. Tätä varten kehitettiin erilaisia suojausmenetelmiä, joita on sen jälkeen pyritty murtamaan vaihtelevalla menestyksellä. Koska kehitys on ollut nopeaa, on eri standardeja käyttävien laitteiden täytynyt olla yhteensopivia toistensa kanssa. Tämä on johtanut siihen, että vaikka jollakin olisi käytössään uusinta tekniikkaa, voi verkossa silti olla toimijoita, joilla on käytössää vanhentunutta laitteistoa. Verkon ollessa yhteensopiva kaikille se voi joutua tietoturvauhkan kohteeksi sen vuoksi, että verkon heikoimman toimijan kautta saatetaan päästä vaikuttamaan myös uudempaa laitteistoa käyttäviä käyttäjiä. Lisäksi isoissa organisaatioissa laitteiston päivityssyklit voivat olla hitaita, jolloin käytössä voi olla pitkäänkin vanhaa laitteistoa, jonka käyttö ei enää ole turvallista.

Laitteisto ei kuitenkaan ole ainut langattoman tietoturvan osa-alue. Käyttäjät muodostavat nykyään jo todennäköisesti suuremman riskin verkkoturvallisuudelle, kuin itse laitteisto ja salausmenetelmät. Verkon huipputeknisestä salauksesta ei ole juurikaan hyötyä, jos käyttäjät eivät osaa käyttää sitä oikein. Varsinkin vanhemman sukupolven voi olla vaikea omaksua uusia toimintatapoja ja ymmärtää vahvojen salasanojen merkitystä. Oman riskinsä muodostaa se, että puolustusvoimien kaltaisessa organisaatiossa on useita järjestelmiä, joihin on lukuisia salasanoja. Tämä johtaa nopeasti siihen, että salasanat ovat jossain kirjoitettuna ylös tai samaa salasanaa käytetään monessa paikassa. Tällaisessa tapauksessa tietoturvariski kasvaa huomattavasti, kun mahdollisen hyökkääjän ei välttämättä muuta tarvitse tehdä, kuin kokeilla yhtä löydettyä salasanaa useampaan paikkaan. Toki täytyy pitää mielessä, että varsinkin puolustusvoimien tapauksessa suurin osa tiloista ja verkoista sijaitsee vartioiduilla alueilla, joka osaltaan vaikeuttaa niihin käsiksi pääsyä.

5.2. Langattoman verkon suojausmenetelmät

Langattoman verkon suojaukseen kuuluu käyttäjien toiminnan ja radiotekniikan lisäksi muutakin. Koska verkkoihin pääsee liittymään kuka vaan, on liittymisen yhteyteen tehty käyttäjän tunnistus. Tunnistuksella varmistetaan, että kyseisellä käyttäjällä on oikeus verkon käyttöön. Tunnistus ei yksinään riitä langattoman tiedonsiirron turvaamiseen, sillä verkkoliikennettä pystytään salakuuntelemaan, vaikka itse yhteyspisteeseen ei oltaisikaan suorassa yhteydessä. Tämän vuoksi verkossa kulkeva liikenne usein salataan erilaisilla salaus algoritmeilla.

Tunnistus on useita, joiden turvallisuus vaihtelee. Periaatteena voidaan pitää, että mitä vanhempaan salaukseen tunnistus liittyy, sitä turvattomampi se on. Yksityiskäytössä ja pienemmissä verkoissa käytetään hyvin usein ennalta jaettua salasanaa, jonka pohjalta tunnistus tapahtuu. Isommissa yhtiöissä on tunnistuspalvelimia, jotka hoitavat verkkoon liittyvien käyttäjien tunnistamisen. Tunnistustapahtumasta ollaan pyritty luomaan sellainen, että se ei itsessään paljasta verkossa käytettäviä salasanoja ja salausavaimia mahdolliselle salakuuntelijalle. Riippuen salaustyypistä, salakuuntelemalla tunnistustapahtuma, voidaan kuitenkin saada selville informaatiota, joka auttaa salasanan murtamisessa. Kaikista heikoin käyttäjän tunnistus on vanhassa WEP-salauksessa, jonka murtaminen vie nykyaikaisella laitteistolla muutamia sekunteja. Tunnistuksen kautta pääsee käsiksi varsinaiseen WEP-avaimeen, jota voidaan sen jälkeen käyttää apuna salatun liikenteen purkuun. Uudemmat WPA ja WPA2-salaukset käyttävät tunnistuksessa niin sanottua neljän suunnan kädenpuristusta, jossa osapuolet varmistavat

toisiltaan, että ne tietävät käytettävän salasanan, mutta eivät paljasta sitä toisilleen. Tällaisessa tapauksessa hyökkääjän on huomattavasti vaikeampaa päästä murtamaan salasanaa. Mikäli koko kädenpuristus saadaan kuunneltua, voidaan salasanaa alkaa murtaa brute force menetelmin, jolloin salasanan löytyminen perustuu joko satunnaisesti, tai ennalta määritellyn kirjaston perusteella suoritettavaan arvaamiseen. Tästä johtuen vahva ja epäjohdonmukainen salasana auttaa suojautumaan mahdollisilta uhkilta kaikista parhaiten.

Sen lisäksi, että käyttäjä tunnistetaan hänen liittyessä verkkoon, myös koko verkkoliikenne salataan. Salaus liittyy läheisesti tunnistamiseen, sillä tunnistamisen yhteydessä vaihdetaan ja luodaan salasanat, joiden perusteella varsinainen salaus tapahtuu. Alkuperäisen WEP-salauksen käyttö ei nykypäivänä enää ole järkevää muualla, kuin sellaisissa tilanteissa, joissa ei ole väliä, mikäli verkon sisältö saadaan selville. Tällaisissa tapauksissa WEP-salauksella saadaan verkosta pidettyä poissa ylimääräiset käyttäjät, jotka muuten kuormittaisivat sitä. Mitään oikeaa suojaa tämä ei kuitenkaan verkolle anna.

WEP-salaukseen luotu TKIP -parannus onnistuu salauksessa hieman paremmin. Sekään ei ole murtovarma, sillä se käyttää edelleen WEP-salauksen pohjana toimivia algoritmeja. TKIP onkin eräänlainen välivaihe, kun on siirrytty AES-salaukseen. Ongelma on jälleen kerran se, että verkot tukevat myös vanhempaa tekniikkaa, jolloin samassa verkossa voi olla laitteita, joissa on AES-suojaus ja vanhoja TKIP-suojausta käyttäviä laitteita. Vaikka uudempien laitteiden kimppuun ei voitaisikaan hyökätä niiden käyttäessä uusinta suojaustekniikkaa, voidaan niiden käyttäjiä kuitenkin häiritä kohdistamalla hyökkäyksen vanhempiin laitteisiin. TKIP:n ongelma on sen MIC -varmenteessa, joka vastatoimenaan katkaisee kaikki yhteydet yhteyspisteeltä, mikäli huomaa lähetettyjen pakettien varmenteissa ongelmia. Tällöin verkossa olevat muut toimija joutuvat myös ulos verkosta. Mikäli hyökkääjä niin haluaa, voi hän jatkaa väärien pakettien lähetystä kaksi kertaa minuutissa, jolloin yhteyspisteen käyttö estyy. TKIP antaa hyökkääjälle helpon keinon suorittaa palvelunestohyökkäys. Kaiken lisäksi TKIP-salauksen pystyy murtamaan, jolloin salattua liikennettä pystytään tulkitsemaan. Tämä ei käy aivan yhtä helposti, kuin WEP-salauksen murtaminen, mutta se on tehtävissä.

Kaikista uusin salausmenetelmä on WPA2 AES, joka on määritelty IEEE:n 802.11i standardissa. Se käyttää 128-bittistä lohkosalausta. Salaus tehdään kierroksissa ja kierrosten määrä riippuu salausavaimen pituudesta. AES-salauksen murtamiseksi ei toistaiseksi ole käytössä kuin brute force menetelmä. Salausavain on kuitenkin niin vaikea murtaa, että se murtamiseen menee todella pitkä aika. Mikäli salasana on oikein tehty ja riittävän pitkä, ei yksi elinikä välttämättä riitä avaimen purkamiseen. Kun ottaa huomioon, että jokaisella kerralla, kun yhteyspisteeseen liitytään, luodaan uudet salausavaimet, ei ole kovinkaan todennäköistä, että saman

istunnon aikana kukaan murtaisi suojausta. AES-suojausta käytettäessä hyökkääjä voi kuitenkin kalastella erilaisia tietoja, joilla salasanan murtamista voidaan yrittää. Verkosta voidaan myös kalastella tietoja erilaisia sivukanavia pitkin, joihin kuuluvat salaukseen käytettävä aika, laitteiden virrankulutus, virheraportit yms. Näitä kanavia pitkin voidaan saada erilaisia tietoja, joista verkkoliikenteen sisältöä voidaan päätellä. Joka tapauksessa helpompi tapa saada tällaisesta verkosta tietoja, on yrittää murtautua sinne toista kautta. Mikäli hyökkääjä onnistuu sovelluskerroksen kautta ujuttamaan käyttäjälle jonkin haittaohjelman, voidaan sen avulla onkia selville käytössä olevia avaimia. Tämä edellyttää kuitenkin käyttäjältä huolimattomuutta.

Yksi mahdollinen vaihtoehto suojata langaton verkkoyhteys on käyttää VPN tunnelia. Mikäli VPN-yhteys on muodostettu oikein, on sitä käytännössä mahdoton murtaa. VPN-yhteyden kanssa käytetään samoja salausmenetelmiä, kuin muissakin langattomissa verkkoyhteyksissä. VPN luo niiden suojaksi vielä erityisen tunnelin, johon pääsee käsiksi vain määritetyt osoitteet.

Kaiken kaikkiaan langattoman verkon suojaus koostuu käyttäjän tunnistuksesta, sen yhteydessä tapahtuvasta salausavainten luonnista ja varsinaisen liikenteen salaamisesta. Käyttäjä tai yritys voi itse päättää, millaista salausta ja tunnistusta tiedonsiirrossaan käyttää, mutta olisi melko merkillistä, mikäli käytössä ei olisi uusin menetelmä. Toki joissain tapauksissa ongelmia voi aiheuttaa vanhentunut laitteisto.

5.3. Langattoman verkon suojaus maantietukikohdassa

Maantietukikohdassa sijaitsevan langattoman verkon käyttöön liittyy muitakin asioita, kuin pelkkä käytettävä salausmenetelmä. Toki on tärkeää, että liikenteen salaaminen ja käyttäjien tunnistaminen tapahtuvat uusimpien mahdollisten menetelmien mukaan, jotta verkkoon ei päästäisi murtautumaan sisälle. Huomioita on kuitenkin kiinnitettävä siihen, kuinka verkko tukikohtaan suunnitellaan. Suunnittelussa tulee ottaa huomioon siihen kohdistuvien uhkien mahdollinen suunta ja aika.

Voi olla hämäävää, kun maantietukikohta perustetaan sisämaahan, ja sinne kohdistuukin yhtäkkiä jokin uhka. Varsinkin, jos tilanne ei ole sodan aika, vaan aivan rauhanomainen harjoitus. Rauhanajan harjoitusta suunniteltaessa olisi hyvä ottaa huomioon mahdollisten verkkohyökkäysten mahdollisuus. Hyökkääjää voi tällaisissa tilanteissa olla lähes mahdotonta löytää, kun paikalla parveilee muutenkin runsaasti siviiliväestöä. On kuitenkin hyvä tiedostaa,

että juuri tämän tyyppisissä harjoituksissa verkkoon kohdistuvan toiminnan suorittaminen on hyökkääjän kannalta kaikista helpointa. Mikäli tukikohtaan on tehty kriisi- ja sotatilanteita varten suunnitelmia, tulisi niihin tehdä jonkin näköinen uhka-arvio verkkoon kohdistuvasta uhkasta. Samalla kun rauhanajan harjoitusta toteutetaan, voitaisiin soveltuvilta osin myös tarkastella ympäristöä uhka-arviota silmällä pitäen. Hyökkääjällä on tuskin rauhan aikana muita tavoitteita kuin tiedustella toimintaa ja maksimissaan kokeilla jotain kevyttä hämmennystä aiheuttavaa toimenpidettä verkkoa kohtaan. Lisäksi verkon rakentamista ja käyttöä harjoiteltaessa kannattaa pitää mielessä, että se on samalla tiedusteltavissa.

Rauhanajan maantietukikohtaharjoituksissa verkon suojaaminen on siis hieman hankalampaa kuin kriisitilanteessa, mutta suojauskeinona voidaan käyttää osaltaan sitä, ettei täydellisiä sodan aikana käytettäviä rakennelmia kokonaisuudessaan rakenneta. Samalla rakennettavien verkkojen sijoittelu ja käyttö kannattaa tehdä tositilanteesta poiketen. Tällä estetään se, että kriisitilanteen tullen maantietukikohdan verkkojen kokoonpano olisi ennalta tiedusteltu. Myös verkon kaavamaista käyttöä tulisi rajoittaa. Mikäli aina tietyn tilanteen tullen verkossa tapahtuu samoja asioita, voidaan siitä helposti päätellä mitä lähetetty data sisältää, vaikka varsinaista salausta ei saataisikaan purettua. Tämä tarkoittaa sitä, että verkon käytölle olisi luotava erillinen suunnitelma, jonka mukaan toimitaan.

Kriisitilanteessa ja sodan aikana tukikohdan suojaaminen on siinä mielessä helpompaa, että käytössä on hyvin todennäköisesti jokin puolustusvoimien omaa toimintaa helpottavaa lainsäädäntöä. Kun maantietukikohtaa aletaan perustamaan, tulisi maastontiedustelun ohessa kiinnittää huomiota kaikkiin, jo paikalla oleviin mastoihin ja antenneihin sillä silmällä, että onko niissä jotain ylimääräistä ja sinne kuulumatonta. Rauhan aikana vihamieliset toimijat ovat hyvinkin voineet käydä lisäämässä paikallisiin mastoihin tai korkeisiin rakennuksiin antennielementtejä, joita siellä ei pitäisi olla. Näiden laitteiden avulla olisi helppoa päästä vaikuttamaan tukikohdan verkkoon. Verkon suunnittelussa on myös hyvä ottaa huomioon näköyhteyden mahdollistaminen vain mahdollisimman pienelle alueelle. Jos antennit saadaan sijoitettua siten, että ne ovat suojaisessa paikassa ja näkevät vain toisensa, voidaan hyvin turvallisesti olettaa, ettei niitä pääse ulkopuoliset kuuntelemaan. Tämä voi kuitenkin muodostua ongelmaksi tukikohta-alueella, joka lähtökohtaisesti on melko tasaisessa maastossa. Langattoman verkon suunnittelussa täytyisi kuitenkin ottaa huomioon ympäröivät alueet muutaman kilometrin säteeltä, jotta voitaisiin kartoittaa paikat, joista tukikohdan verkkoa vastaan voitaisiin toimia. Näitä paikkoja tulisi sitten aika-ajoin tarkastaa, jotta mahdolliset vihamieliset toimijat saataisiin kiinni.

Olemassa olevat tekniset ratkaisut ovat riittäviä tukikohdan verkossa liikkuvan datan salaamiseen, mikäli käytössä on uusinta salaustekniikkaa käyttävää laitteistoa. On kuitenkin todettava, että esimerkiksi palvelunestohyökkäyksiä ja häirintää vastaan toimiminen on hankalaa, vaikka itse liikuteltava data olisikin turvassa. Myös reagoiminen tietynlaiseen hyökkäämiseen voi paljastaa hyökkääjälle sen vaikutuksia, joita ei välttämättä haluta paljastaa. Verkon käytössä on myös huomioitava sen käytön ajoittaminen. Aina kun verkkoa käytetään, se säteilee ja sitä voidaan salakuunnella. Vaikka varsinaista dataa ei saataisikaan purettua, voi verkon käyttö paljastaa tiettyjä toimintatapoja tai menetelmiä, joita vastustaja voi hyväksikäyttää jossain myöhemmässä tilanteessa.

Sen lisäksi, että maantietukikohdassa kiinnitetään huomiota verkon fyysisiin rakenteisiin, ympäröivään maastoon ja salauksen tekniseen toteutukseen, olisi myös hyvä kiinnittää huomiota inhimilliseen puoleen. Verkon käyttäjät ovat kaikki ihmisiä, joilla voi olla erilainen tietotaito laitteiden käytöstä ja ennen kaikkea tietoturvasta. Tämän vuoksi olisikin järkevää, jos kaikki tukikohdassa toimivat joukot joutuisivat käymään langattomien verkkojen käyttöön liittyen tietoturvakoulutusta. Tällaisissa tapahtumissa voitaisiin demonstroida, kuinka langattomaan verkkoon voidaan murtautua ja mitä tietoja sieltä voidaan kalastella. Pelkästään verkkopohjaisia rasti ruutuun toteutuksella tehtyjä oppimispaketteja täyttämällä ei välttämättä kaikille avaudu se, kuinka monimutkainen aihe langaton tietoturva oikeasti on.

Tulevaisuudessa liikkuminen tulee todennäköisesti lisääntymään ja vanhanaikaisten langallisten verkkojen vetäminen alkaa olla niin hidasta, että se voi jarruttaa toimintaa. Tällöin langattomien verkkojen käyttö vain korostuu ja samalla korostuu niiden oikeaoppinen rakentaminen ja suojaaminen. Perinteinen kehäajattelu maantietukikohdan suojaamisessa toimii langattomalla aikakaudellakin siinä mielessä, että sillä pidetään vihamieliset tahot mahdollisimman kaukana suojattavasta alueesta. Ilmateitse liikkuvaa signaalia ei kuitenkaan voi varsinaisesti suojata perustamalla suojakehää, koska signaalin vaimenemisesta johtuen kehä saattaisi olla käytettävien resurssien puitteissa liian iso. Sen sijaa pitäisi siirtää ajattelua siihen suuntaan, että jokaiselta paikalta, johon on tarkoitus perustaa yhtään pidempiaikaista verkkotoimintaa, tulisi määritellä maaston perusteella parhaat mahdolliset paikat omille yhteyspisteille ja linkeille. Vastaavasti tulisi tiedustella tarvittavan laajalla säteellä ympäristöstä sellaiset sijainnit, jotka soveltuvat verkkoa vastaan suoritettavalle toiminnalle. Näitä paikkoja ei ole välttämätöntä suojata jatkuvasti, vaan niiden suojaus tulee toteuttaa riittävän pienillä sykleillä, jolloin sieltä ei ehditä vaikuttamaan tukikohdan toimintaan. Lisäksi perustettavan tukikohdan alueella tulisi pystyä suorittamaan ennakoivaa tiedustelua riittävän aikaisin, jotta alueen turvallisuudesta voidaan varmistua.

5.4. Jatkotutkimuksen aiheita

Mahdollisia jatkotutkimusaiheita maantietukikohdan langattomaan verkkoon kohdistuvia uhkia vastaan voisivat olla käytännön tutkimukset. Tällöin voitaisiin luoda kokeellinen ympäristö, jossa olisi langaton verkko, jonka suojausmenetelmiä voitaisiin vaihtaa. Verkon voisi sijoittaa oikeaan maastoon, jolloin voitaisiin tutkia sitä, kuinka kaukaa sen pystyy oikeasti havaitsemaan ja salakuuntelemaan. Lisäksi verkon eri suojausmenetelmiä vastaan voitaisiin suorittaa hyökkäyksiä, joilla voitaisiin todeta teorian paikkansapitävyys. Myöhemmässä vaiheessa tällainen verkkohyökkäysskenaario voitaisiin liittää johonkin harjoitukseen, jolloin päästäisiin kokeilemaan konkreettisesti sitä, kuinka mahdollista verkon salakuuntelu ja sitä vastaan hyökkääminen on, kun vastassa on hyökkääjän näkökulmasta vihamielistä toimintaa. Tutkimuksessa voitaisiin kerätä dataa ja yrittää analysoida sitä siten, että siitä olisi hyötyä kuvitteellisiin jatkotilanteisiin. Vaikka itse salausta ei saataisikaan murrettua, voitaisiin olemassa olevaa dataa pyrkiä käyttämään hyväksi, kun verkkoja ja niiden käyttöä suunnitellaan.

LYHENTEET

Lyhenne	Kuvaus
AES	Advanced encryption standard
APR	Addres Resolution Protocol
BSPK	Binary Phase Shift Keying
CCK	Complementary Code Keying
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access With Collision Detection
CTS	Cleared To Send
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ESP	Encapsulating Security Payload
FMS	Fluhrer, Mantin and Shamir
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key-Exchange
IP	Internet Protocol
IPsec	IP Security Architecture
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logic Link Control
LOS	Line Of Sight
MAC	Media Access Control
MIC	Message Integrity Check
MIMO	Multiple-Input, Multiple-Output

MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAV	Network Allocation Vector
OFDM	Orthogonal frequency-division multiplexing
OSI	Open Systems Interconnection
PCF	Point Coordination function
PIFS	PCF Interframe Space
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
PPDU	PLCP Protocol Data Unit
PTW	Pychkine Tews Weinmann
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial In User Service
RTS	Request To Send
SIFS	Short Interframe Space
SNAP	Subnetwork Access Protocol
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol / Internet Protocol
TKIP	Temporal Key Integrity Protocol
TSC	TKIP Sequence Counter
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
VPN	Virtual Private Network

LÄHTEET

[1] 802.11 MAC series – Basics of MAC Architecture. https://www.cwnp.com/802.11-mac-series-ndash-basics-mac-architecture-ndash-part-1-3/

[2] 802.11 PHY Layers, CWAP. http://media.techtarget.com/searchMobileComputing/downloads/CWAP_ch8.pdf

[3] 802.11i Authentication and Key Management White Paper, Planet3 Wireless Inc. https://www.cwnp.com/uploads/802-11i_key_management.pdf

[4] 802.11n Primer, airmagnet 2008. http://dl.aircrack-ng.org/wiki-files/doc/wireless_basics_and_tutorials/WP-802.11nPrimer.pdf

[5] Advanced Encryption Standard. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[6] An Overview of 802.11 Wireless Network Security Standards & Mechanisms, SANS Institute InfoSec Reading Room. https://www.sans.org/reading-room/whitepapers/wireless/overview-80211-wireless-network-security-standards-mechanisms-1530

[7] An Overview of Cryptanalysis Research for the Advanced Encryption Standard. Alan Kaminsky, Michael Kurdziel ja Stanislaw Radziszowsky. https://www.cs.rit.edu/~spr/PUBL/aes.pdf

[8] Antenna Basics, wireless ICTP. http://wireless.ictp.it/handbook/C4.pdf

[9] Authentication Types for Wireless Devices, CISCO. http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html

[10] Break WEP Faster with Statistical Analysis, Rafik Chaaboumi School of computer and communication Sciences 2006. https://lasec.epfl.ch/pub/lasec/doc/cha06.pdf

[11] Cache-Collision Timing Attacks Against AES, Joseph Bonneau ja Ilya Mironov 2006. http://www.jbonneau.com/doc/BM06-CHES-aes_cache_timing.pdf

[12] Cryptanalysis of IEEE 802.11i TIKP, Finn Michael Halvorsen ja Olav Haugen, NTNU 2009. http://wiki-files.aircrack-ng.org/doc/tkip_master.pdf

[13] CWAP - 802.11 Data: Frame Aggregation. https://mrncciew.com/2014/11/01/cwap-802-11-data-frame-aggregation/

[14] Differential Power Analysis attacks on AES, Kevin Meritt 2012. https://people.rit.edu/kjm5923/DPA_attacks_on_AES.pdf

[15] Digitaalinen taistelukenttä kolmas painos, Jyri Kosola ja Tero Solante 2013.

[16] Frame structure, School of computer science, lecture 6, http://www.cs.mcgill.ca/~cs535/lect_notes/Lecture6.pdf

[17] Fresnel Zone. https://en.wikipedia.org/wiki/Fresnel_zone

[18] Google maps

[19] Guide to IPsec VPNs, NIST 2005. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

[20] Hacking Exposed Wireless 2nd edition, Johnny Cache, Joshua Wright ja Vincent Liu 2010.

[21] IEEE 802.11g-2003. https://en.wikipedia.org/wiki/IEEE_802.11g-2003

[22] IEEE 802.11n Part11: Wireless LAN Medium Access Control(MAC) and Physical Layer (Phy) Specifications, IEEE Computer Society 2009.

[23] IEEE 802.11n-2009. https://en.wikipedia.org/wiki/IEEE_802.11n-2009

[24] IPsec VPN WAN Design Overview, CISCO systems Inc. 2007. https://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f22f.pdf

[25] Kansalaisen karttapaikka. https://asiointi.maanmittauslaitos.fi/karttapaikka/

[26] Käyttötapaus (use case). https://fnoll.wordpress.com/2012/08/20/kayttotapaus-use-case/

[27] Langattomat Lähiverkot, Matti Puska 2005.

[28] Non-broadcast Wireless Networks with Microsoft Windows, Microsoft support. https://technet.microsoft.com/en-us/library/bb726942.aspx

[29] OSI model Microsoft support. https://support.microsoft.com/fi-fi/help/103884/the-osi-model-s-seven-layers-defined-and-functions-explained

[30] OSI model. https://en.wikipedia.org/wiki/OSI_model

[31] Practical attacks against WEP and WPA, Martin Beck ja Erik Tews 2008. https://dl.aircrack-ng.org/breakingwepandwpa.pdf

[32] Practical Verification of WPA-TIKP Vulnerabilities, Mathy Vanhoef ja Frank Piessens.
https://pdfs.semanticscholar.org/1a9d/6f6d7760eaf22e438eed3861b52e44069129.pdf

[33] Side-Channel Analysis Resistant Implementation of AES on Automotive Processors, Andreas Hoheisel 2009.
https://www.emsec.rub.de/media/crypto/attachments/files/2010/04/ms_hoheisel.pdf

[34] Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, YongBin Zhou, DengGuo Feng.
http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf

[35] Tekniset tutkimusmenetelmät maanpuolustuskorkeakoulussa, Esa Lappalainen ja Jorma Jormakka 2005.

[36] The Advanced Encryption Standard Chapter 7.
http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

[37] Valmiuslaki ja Poikkeustilalaki, Finlex

[38] Virtual Private Networking Basics, Netgear Inc. 2005.
http://documentation.netgear.com/reference/fra/vpn/pdfs/FullManual.pdf

[39] Wi-Fi: Overview of the 802.11 Physical Layer and Transmitting Measurements Primer, Tektronix. http://www.nortelcoelectronics.se/document-file5116?lcid=1053&pid=Native-ContentFile-File

[40] Wireless Security and the IEEE 802.11 Standards, GIAC Essentials.
https://www.giac.org/paper/gsec/4214/wireless-security-ieee-80211-standards/106760

[41] WLAN. https://en.wikipedia.org/wiki/Wireless_LAN

[42] WPA password cracking parallel processing on the Cell BE, Martin Daniel 2009.
http://projekter.aau.dk/projekter/files/17901417/WPA_password_cracking__Parallel_processing_on_the_Cell_BE_-goup1045.pdf